Defense Exportability Integration Best Practices Job Support Tool (JST)

Overview

This Job Support Tool (JST) describes Defense Exportability Integration (DEI) best practices that Program Management Offices (PMOs) and supporting functional organizations should consider using based on DoD 5000 series policy and the defense exportability guidance contained in the Guide to DoD International Acquisition and Exportability (IA&E) Practices (IA&E Guidebook). This JST is designed to help PMOs, the international manager, and supporting functional organizations plan and execute program-level DEI activities that lead to achievement of their programs' IA&E objectives.

The IA&E Guidebook emphasizes the importance of PMO-led DEI efforts that provide a solid foundation for all types of international acquisition activities including International Cooperative Programs (ICPs), Foreign Military Sales (FMS), Direct Commercial Sales (DCS), Building Partner Capacity (BPC), and international contracting. Comprehensive DEI planning and execution throughout the program life cycle leads to enhanced acquisition outcomes and security cooperation relationships that support U.S., allied, and friendly nations' warfighters. Failure to adequately address DEI considerations can negatively impact the benefits gained from international acquisition programs for both the U.S. and partner/customer.

The overall goal of DEI policies and procedures is to achieve an optimal balance among key U.S. national security and foreign policy goals; a) building coalition partner operational capability; b) reducing overall acquisition costs; c) engaging the global defense technology base while maintaining U.S. military technological edge; d) establishing and strengthening political-military relationships; and e) strengthening the domestic and allied industrial base.

Achieving a balance among often-competing international acquisition goals at the individual program level can be incredibly challenging. PMOs often find Technology Security and Foreign Disclosure (TSFD) processes and export control-related efforts vexing since they do not have a single DoD process owner. The TSFD "system" involves overlapping responsibilities among a semi-autonomous collection of various TSFD processes – colloquially referred to as the TSFD "Pipes" (see IA&E Guidebook, Section 1-9 for details) – which issue both broad and specific TSFD policy guidance applicable to all OSD and DoD Component international acquisition activities. These TSFD "pipes" operate outside the DoD Component Acquisition Executive (CAE), the Office of the Under Secretary of Defense for Acquisition and Sustainment's (OUSD(A&S)) – and in some cases, the DoD -- span of control, which further exacerbates the complexities that PMOs often encounter in obtaining required TSFD approvals relevant to their program.

Organization

This JST, which is designed to augment DoD 5000 series policy and the IA&E Guidebook, provides best practice information in DEI areas, with special emphasis on PMO-led DEI activities, and is organized in six sections as shown in Figure 1.

Figure 1: DEI Best Practices Process Overview

Section	Description
1	Fundamental Policies
2	Program Protection (International Considerations)
3	Navigating the Technology Security & Foreign Disclosure (TSFD) "Pipes"
4	Exportability Design & Development
5	International Security and Export Control Considerations
6	Exportability Integration
Appendix A	Defense Exportability Roadmap Sample Template

NOTE

PMOs with international acquisition responsibilities should work closely with their local Foreign Disclosure Office (FDO), their DoD Component International Program Organization (IPO), and other DoD Component and Office of Secretary of Defense (OSD) level organizations, as applicable, to organize, plan, and implement program-specific DEI efforts.

Relationship to Other JSTs

For new acquisition programs, IA&E Guidebook Section 1-3 recommends that Program Managers conduct an IA&E Assessment to collect information and assess factors related to a program's future international involvement, including DEI considerations. Please refer to the IA&E Assessment JST for best practice DEI guidance in this area. The Acquisition Strategy – International Considerations JST provides additional best practice guidance regarding DoD documentation requirements for the DEI aspects of international involvement in DoD acquisition programs throughout a program's life-cycle. Depending on the nature of their programs, PMOs should also consider consulting the International Cooperative Program (ICP) JST or Foreign Military Sales (FMS) Systems Acquisition JST to help address the DEI aspects of current and future ICP and FMS arrangements. For mature programs with substantial international acquisition, involvement – including complex DEI planning and implementation challenges – consult the International Business Planning JST

Section 1 – Fundamental Policies

A. Policy References

1. Program Protection Policy

DoDI 5000.83, Technology and Program Protection to Maintain Technological Advantage" and Section 2.B. (Defense Exportability and Program Protection Considerations) of the IA&E Assessment JST provide DoD acquisition policy and recommended best practices that govern the international aspects of program protection.

2. General Acquisition Policy

In support of top level strategic guidance regarding partnerships, alliances and facing shared challenges with similarly minded nations, DoDD 5000.01, paragraph 1.2.t. requires DoD acquisition programs to plan for coalition partners and to consider incorporation of exportability features in the early design and development phase of acquisition programs' acquisition strategies. DoDI 5000.02, paragraph 4.1.b.(2) requires Program Managers to 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. The Adaptive Acquisition Framework (AAF) in DoDI 5000.02 contains six acquisition pathways: Urgent Capability Acquisition, Middle Tier of Acquisition (MTA), Major

Capability Acquisition (MCA), Software Acquisition, Defense Business Systems, and Acquisition of Services. Planning for international involvement in a program is required in the MCA pathway (see DoDI 5000.85, Appendix 3C.4.) and may be required in the MTA pathway rapid fielding efforts (see DoDI 5000.80, paragraph 3.2.d).

3. Building in Exportability

DoD's general acquisition policy places particular emphasis on the importance of building exportability into DoD's new and modified major capability systems consistent with the U.S. Government (USG) Conventional Arms Transfer (CAT) Policy implementation guidance in this area. DoDI 5000.85, paragraph 3C.4. requires PMs to integrate IA&E planning into the program's acquisition strategy beginning at the entry milestone and continuing through all phases of the acquisition process and to design the system for exportability to foreign partners. PMs must plan for the demand and likelihood of cooperative development or production, and foreign sales (e.g., Direct Commercial Sales or Foreign Military Sales) early in the acquisition process, and consider U.S. export control laws, regulations, and DoD policy for foreign transfers when formulating and executing the acquisition strategy in accordance with DoDI 2040.02, PMs must also pursue cooperative opportunities and international involvement throughout the acquisition life cycle to enhance international cooperation and improve interoperability in accordance with DoDI 2010.06.

Program managers should assess any allied/partner interoperability and coalition partner-related JCIDS Initial Capabilities Document (ICD) and Capability Development Document (CDD) requirements established in JROCM 025-19 based on the guidance contained in the JCIDS Manual, then take appropriate steps to develop initial defense exportability-related program protection measures based on ICD and CDD requirements to support future sale, transfer, or use of the system to allied/partner nations. A summary of the JCIDS Manual's Defense Exportability Guidance is available on the DAU.edu International Acquisition Management Community of Practice (ICOP) website.

In addition to any exportability requirements established in ICDs and CDDs, program managers are also responsible for establishing overall exportability requirements in an MCA program's Acquisition Strategy per DoDI 5000.85, paragraph 3C4.. PMs for MDAPs that elect to pursue a U.S.-only design and not plan for system export require an MDA-approved exportability design waiver which must be reviewed at each milestone per DoDI 5000.85, paragraph 3C.4.a.(1). If a program has been approved for a waiver for a U.S.-only design, the MDA for the program is required to notify the USD(A&S) and the DoD JROC requirements validation authority.

4. IA&E Laws, Regulations, & Policies Reference List

Consult the DAU.mil website's International Acquisition Management (IAM) Community of Practice (ICOP) website for a comprehensive IA&E Laws, Regulations, & Policies Reference List.

Section 2 – Program Protection (International Considerations)

A. Program Protection Overview

Program protection measures are one of the two foundational "building blocks" for PMO-level DEI efforts (TSFD processes represent the second foundational building block). DoDI 5000.83 establishes policy, assigns responsibilities, and provides procedures for Science and Technology (S&T) managers and lead systems engineers to manage system security and cybersecurity technical risks resulting from various types of omnidirectional threats in order to develop and implement measures to protect:

- DoD-sponsored research and technology that is in the interest of national security
- DoD warfighting capabilities

The table below provides an overview of how DoDI 5000.83 policy impacts overall DoD acquisition program protection activities throughout the DoD acquisition life cycle:

Program Projection Efforts	S&T-RDT&E Tech Base Activities (1)	ATD-Prototype RDT&E Activities (2)	Acquisition Program RDT&E Activities (3)
Who Leads	S&T Managers	Mix of S&T Mgrs, Lab Engineers, and System Engineers	Lead System Engineers supporting Program Managers (PMs)
Primary Focus	Establish S&T Tech Area Program Protection Plans (TAPPs)	Establish/implement S&T Projection Plans for specific projects	Establish/implement Program Protection Plans (PPPs) for specific programs.
Desired Outcome	Ensure existing and emerging new/evolving tech is protected	Ensure transitioning new/evolving tech is protected at the project level	Ensure fielded new/evolving tech is protected in fielded and deployed systems

(1) DoD Science & Technology (S&T) activities – which are aligned with the RDT&E Budget Activities (BAs) 6.1. and 6.2 per the DoD Financial Management Regulations, Volume 2B, Chapter 5, para 1.5) – are conducted independent of DoD acquisition program RDT&E efforts.
(2) DoD Advanced Technology Development (ATD) activities – which are aligned with RDT&E Bas 6.3 and 6.4 – that focus on transition of new technology into DoD acquisition programs.
(3) DoD Acquisition RDT&E activities – which are aligned with RDT&E Bas 6.4, 6.5, and 6.7 -- that focus integration of new technology into new or existing DoD systems and equipment that is fielded and used by DoD operational forces.
(4) This includes the entire range of DoD AAF) acquisition efforts, including Urgent Capability Acquisition (DoDI 5000.81), Middle Tier of Acquisition (DoDI 5000.80), and Major Capability Acquisition (DoDI 5000.85) efforts.

B. Program Protection Pillars

Planning and execution of protection measures based on overall DoDI 5000.83 guidance in key program protection areas (Cybersecurity, Communications Security (COMSEC), Critical Program Information & Critical Components (CPI/CC), and Trusted Systems and Networks (TSN)) should address both U.S. domestic and international acquisition aspects.

The following table provides a look at these key areas, the elements the U.S. wants to protect, and the type of protection measures used to ensure their security.

Cybersecurity/COMSEC	CPI/CC	TSN
Classified Military Information (CMI) and Controlled Unclassified Information (CUI) resident in & transmitted by DoD government & industry program teams, systems & support systems, operational networks, and general IT networks	Operational system and support system elements (e.g., software algorithms and specific hardware residing on the system/support system) that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence	Information and technology (hardware, software, firmware) that deliver or protect mission critical functionality of a system or may introduce vulnerability to the mission critical functions of an applicable system
Overall program physical, cybersecurity & COMSEC protection measures	Anti-Tamper (AT) and Differential Capability (DC) protection measures	Software and hardware assurance and supply chain risk management protection measures

- **Identification and protection of program information**, in particular Classified Military Information (CMI) and Controlled Unclassified Information (CUI)) that is resident in the operational system and its product support system that is protected by Cybersecurity, Communications Security (COMSEC), information security, and physical security measures.
- **Identification and protection of the operational system and its product support system's Critical Program Information (CPI) and Critical Components (CCs)**. CPI/CCs will be identified early and reassessed throughout the RDT&E program so that CPI/CC protection requirements and countermeasures may be identified and applied as the CPI/CCs are developed and modified throughout the lifecycle as needed. CPI/CCs are primarily protected by Anti-Tamper (AT) and Differential Capability (DC) protection measures. CPI/CC protection measures will be integrated and synchronized, then documented in the Program Protection Plan (PPP) as required by (DoDI 5200.39, paragraph 3). Once their program's CPI/CCs have been defined, program managers will use their PPP to describe the program's CPI/CCs; address the threats to and vulnerabilities of these items; plan for the development and implementation of specific countermeasures to mitigate associated risks; and address exportability design considerations related to the program protection aspects of potential foreign involvement.

  Differential Capability is modifying or removing technologies and/or capabilities from DoD systems not authorized for export resulting in one or more exportable versions, as well as incorporating capabilities specifically requested by the foreign nation that are not included in the U.S. version of the system.

  Anti-Tamper is program design, development, and security efforts intended to prevent or delay exploitation of CMI/CUI and CPI/CC in DoD systems and networks, thereby impeding countermeasure development, unintended technology transfer, and reverse engineering.

- Identification and protection of Trusted Systems & Networks (TSN) critical components which contain information and communications technology (ICT). TSN critical components include hardware, software, and firmware, whether custom, commercial, or otherwise developed, which deliver or protect mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system. Program managers should take steps to protect the operational system and its product support system's TSN mission-critical elements and components through measures such as Systems Security Engineering (SSE), Supply Chain Risk Management (SCRM), Anti-Counterfeits, Hardware & Software Assurance, and Trusted Foundry.

Each one of these program protection areas is governed by a separate set of organizations, policies, and practices. Consult IA&E Guidebook, Section 1-10 for Program Protection Activities and the DAU ICOP website's IA&E Laws, Regulations, & Policies Reference List which provides specific guidance documents that govern DoD program protection activities. The PMO and its functional support personnel should engage subject matter experts in all of these areas to develop comprehensive, harmonized domestic and international program protection measures:

- DoD Chief Information Officer (CIO), National Security Agency (NSA), CYBERCOM, USD(Intelligence & Security), and the Defense Counterintelligence and Security Agency (DCSA) are responsible for the ***Cybersecurity and Information Security*** areas based on DoDI 5000.90 and DoD 8500 series policy guidance, and DoD 5200 series Information Security Program guidance
- Office of the Under Secretary of Defense for Research & Engineering (OUSD(R&E)) and the DoD Anti-Tamper Executive Agent (ATEA) are responsible for governance of the ***CPI/CC Protection*** area based on DoDD 5200.47E, DoDI 5200.39, and the DoD Technology and Program Protection (TPP) Guidebook. SAF/AQLS is designated as the DoD Anti-Tamper Executive Agent (DoD ATEA)

- OUSD(A&S), in coordination with the DoD CIO, oversees the implementation of, and issue supporting guidance as necessary, in support of the ***TSN Protection*** area based on DoDI 5200.44 and the TPP Guidebook.

C. Life-Cycle Program Protection Aspects

The domestic and international aspects of program protection described in DoDI 5000.83 and the TPP Guidebook should be addressed from the program's inception throughout the acquisition life cycle to achieve optimal technology and program protection.

Program Protection Plans (PPPs) developed for acquisition programs will be based on any relevant Technology Area Protection Plans (TAPPs), implemented through corresponding S&T Protection Plans, as well as any "three pillars" aspects that require development and implementation of program-specific protection measures.

- TAPPs will be established and maintained by USD(R&E) for each S&T modernization priority area. They will inform S&T research at the appropriate BA level, or at Technology Readiness Levels 1-6 and PPPs. They will be designed to reduce compromise or loss of critical technologies and protect against unwanted technology transfer and used to guide DoD acquisition efforts in: S&T; export controls; international agreements; security; counterintelligence; and U.S. law enforcement activities.
- S&T Managers in the DoD Components will prepare S&T Protection Plans as a management tool to guide S&T protection activities at the S&T and RDT&E project level. Such projects, when associated with critical technology or modernization priority areas, will need to develop an S&T Protection Plan that includes critical technology elements and enabling technologies; threats to, and vulnerabilities of, these items; and selected countermeasures to mitigate associated risks. These S&T Protection Plans will be submitted for approval before each S&T/RDT&E project's approval – and updated, as appropriate -- based on procedures defined by each DoD Component.

The PMOs in DoD acquisition programs, supported by the Systems Engineering (SE) and Systems Security Engineering (SSE) functional personnel working with other key functional organizations (e.g., international manager, FDO, security manager), and the contractor team should review and apply relevant TAPPs and S&T Program Protection Plans to plan and implement the following international aspects of program protection:

- Applicable USG/DoD TSFD and export control policy is understood and implemented in the system's exportable version(s)
- TSFD and export control policy-driven Differential Capability (DC) requirements that lead to development of one or more exportable versions of the system are developed based on OUSD(A&S) Defense Exportability Features (DEF) policy guidance and Section 4 of this JST
- ***Cybersecurity and Information Security*** protection measures associated with potential ICP, FMS, DCS, or BPC arrangements should be developed to ensure future materiel and operational interoperability with allied and friendly nations who purchase the system and/or participate in coalition or multinational operations with U.S. forces operating the system
- For identified Critical Program Information/Critical Components (***CPI/CC)***:
    - All CPI contained in domestic and exportable versions is identified and adequately protected by AT
    - Conduct a horizontal protection analysis (see TPP Guidebook, Section 3.4.3, "Horizontal Protection of CPI") to ensure CPI associated with more than one program is be protected to the same degree. Any CPI and AT resulting from TSFD and export control policy-driven DC modifications in the export version(s) should be evaluated by the PMO, key functional organizations, and the DoD ATEA. Addressing AT requirements moves rapidly into discussion of classified information. Programs should contact the DoD ATEA for appropriate guidance before drafting any AT-related documents.

- As the system matures, ***CPIC/CC*** protection measures should be periodically reassessed to take into account diminishing manufacturing sources and materiel shortages and parts obsolescence-related configuration changes -- as well as the evolution of sustainment and spares management activities -- throughout the program's life cycle. Any potentially adverse impacts identified by CPI reassessment efforts should be addressed, as appropriate, through development and implementation of modified/new program protection measures. ***TSN*** protection measures associated with potential ICP, FMS, DCS, or BPC arrangements with other nations should be developed to ensure that the TSN aspects of both domestic and exportable versions achieve an adequate level of protection.
- DoD domestic and international security arrangements and USG export controls govern the export and import of DoD information and supply chain components by U.S. and foreign industry for both domestic and international versions of a system. Overall system program protection measures for all program protection areas should be harmonized and integrated in the program's international security and export control execution (See Section 5 of this JST for details.)

D. Domestic and International Program Protection Integration

PMOs should plan and implement integrated domestic and international program protection measures from the program's inception recognizing that – analogous to establishment and development of system interoperability aspects – "perfect information" will not be available to achieve "100% solutions" during a program's initial stages. Establishment of reasonable, initially achievable domestic and international program protection measures early in the program's life cycle provides a solid foundation for program-specific initial DEF feasibility study efforts. As the program matures, combined program protection and DEF measures (see Section 4 for details) should lead to development and fielding of affordable exportable versions that optimally protect leading edge DoD capabilities and technologies.

E. Analysis & Evaluation -- Key Areas

During the initial planning stages of Defense Exportability Integration efforts, PMOs, international managers, and supporting functional organizations should carefully assess the following key considerations:

1. Comprehensive TSFD Engagement

- Have all relevant Technology Security and Foreign Disclosure (TSFD) channels been actively engaged to ensure the development and implementation of comprehensive and cohesive program protection measures for both U.S. and exportable system versions, aligning with international requirements?

2. Future Exportable Variants Planning

- In accordance with applicable TSFD guidance, have plans been set in motion to establish program protection measures for future exportable variants, rather than focusing solely on measures for U.S.-only systems?

3. Collaborative Trade-Off Assessment

- Are your Systems Engineering (SE) and Systems Security Engineering (SSE) functional personnel collaborating effectively with other critical functional entities, such as the PMO, international manager, Foreign Disclosure Officer (FDO), security manager, and contractor team?
- Are they collectively evaluating and implementing domestic and international trade-offs to formulate program protection measures that are both effective and cost-efficient for both U.S. and exportable versions of the system?

4. Integrated Design Approach

- Have you and your functional support teams adopted a DEF design approach that integrates program protection measures and adheres to TSFD and export control policy-driven Differential Capability (DC) requirements?

- Is this approach expected to lead to the development of one or more exportable versions of the system?
- If not, what specific obstacles have been encountered, and what actions are being taken to address and resolve them?

5. Program Protection Plan Coverage

- Have you and your functional support personnel addressed the domestic and international dimensions of all program protection areas in the Program Protection Plan (PPP) right from the program's inception and through subsequent acquisition phase activities, including program upgrades and sustainment? (Refer to IA&E Guidebook Section 1-10 for detailed guidance on this matter.)

Section 3 – Navigating the TSFD "Pipes"

A. TSFD Overview

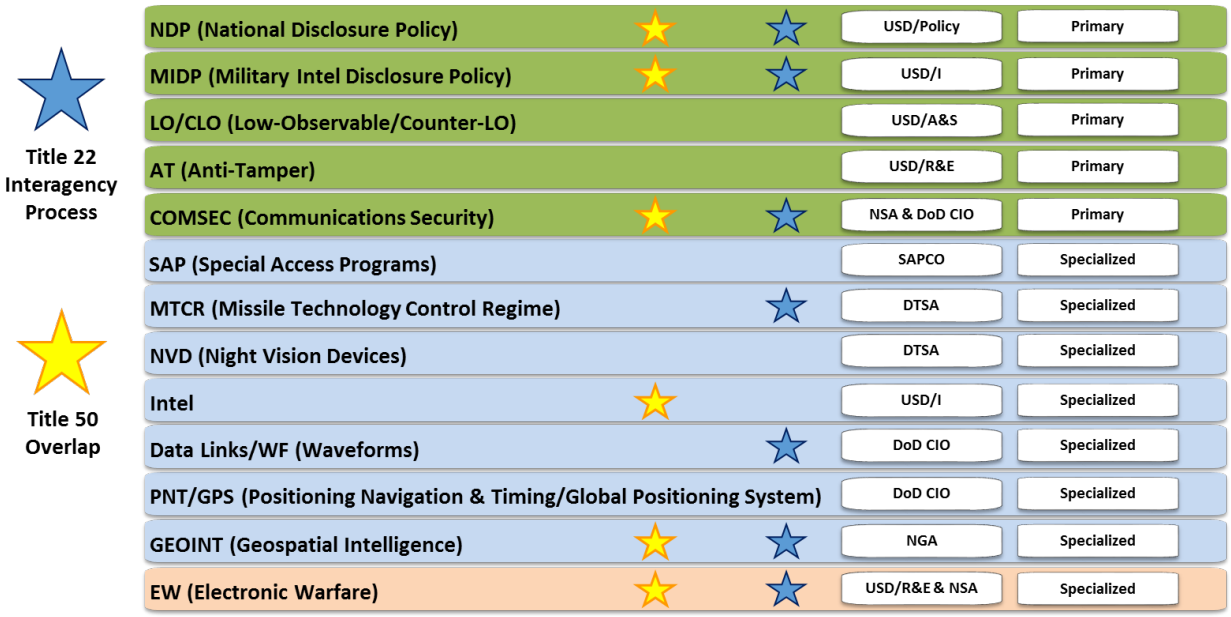
TSFD is the second foundational building block upon which PMO-level DEI efforts are based. Unlike program protection, which has both a domestic and international aspects, the USG/DoD TSFD evaluation and decision-making processes -- commonly referred to as "navigating the TSFD pipes" -- focus on the potential benefits and risks associated with proposed international acquisition activities in their respective areas of responsibility.

B. TSFD Pipe Navigation Best Practices

Step 1 - Assessment and Identification

PMO's, in consultation with their DoD Component IPO and FDO, should identify the applicable TSFD pipes that pertain to their program as early as possible in the DoD acquisition process. (See Figure 2 below as well as the IA&E Guidebook Section 1-9 for details.) Programs in Materiel Solution Analysis (MSA) or Technology Maturation and Risk Reduction (TMRR) phases should conduct an initial DEF Feasibility Study as part of their IA&E Assessment and in developing their Acquisition Strategy in order to systematically evaluate which TSFD pipe policy guidance may be pertinent to future program ICP, FMS, DCS, or BPC efforts. Programs in later acquisition phases should conduct a DEF Feasibility Study that identifies and documents program-related TSFD pipe policy guidance that has already been issued. Then assess the need for additional TSFD pipe engagement, to ensure the PMO adequately considers the breadth and depth of USG/DoD TSFD policy decision making required to execute the international aspects of the program's Acquisition Strategy and International Business Plan (IBP).

Figure 2: Technology Security and Foreign Disclosure Processes



Primary DoD Processes (green)

1. National Disclosure Policy (**NDP**) governs the release of Classified Military Information (CMI) through the National Disclosure Policy Committee (NDPC) for CMI Categories 1-7; chaired by Director, Defense Technology Security Administration (DTSA)
2. Military Intelligence Disclosure Policy (**MIDP**) governs the release of CMI Category 8 (Military Intelligence); chaired by USD(I)
3. Low Observable and Counter Low Observable (**LO/CLO**) process governs release of LO/CLO capabilities and technologies under the leadership of USD(A&S). A&S's Director, Special Projects chairs the Tri-Service Committee that supports the LO/CLO Executive Committee (LO/CLO EXCOM), chaired by USD(A&S)
4. Anti-Tamper (**AT**) process governs the protection of CPI under the leadership of USD(R&E) through the LO/CLO Executive Committee (EXCOM), DoD AT Executive Agent (ATEA) and DoD Component AT organizations
5. Communications Security (**COMSEC**) process governs the release of USG communications security capabilities and technologies through the USG-level Committee for National Security Systems (CNSS) which is chaired by the National Security Agency (NSA)

Specialized DoD Processes (blue)

1. Special Access Programs (**SAP**) process governs release of DoD SAP capabilities and technology through the DoD Special Access Program Coordinator (SAPCO) (A&S's Director, Special Program's "other hat") through the SAP Oversight Committee (SAPOC), under the leadership of DepSecDef
2. Missile Technology Control Regime (**MTCR**) process governs export of "missile system" (including unmanned aerial system) capabilities and technologies for "missile systems" with the potential to deliver weapons of mass destruction under the leadership of the State Department (OUSD(P)/DTSA is the DoD representative in this process)
3. Night Vision Device (**NVD**) technology release process governs release of NVD capabilities and technologies under the leadership of OUSD(P)/DTSA

4. Intelligence (**Intel**) processes (various) govern release of USG and DoD intelligence products led by the Director of National Intelligence (DNI). OUSD(I) is the DoD representative in the process supported by the Defense Intelligence Agency (DIA)
5. Data Link/Waveform (**DL/WF**) process governs release of DoD DL/WF capabilities and technology under the leadership of DoD Chief Information Officer (CIO)
6. Positioning, Navigation, and Timing (**PNT**)/Global Positioning System (**GPS**) process governs release of specialized USG PNT/GPS capabilities and technology under the leadership of DoD CIO
7. Geospatial Intelligence (**GEOINT**) process governs the release of GEOINT products (including specialized mapping data) through the USG-level Remote Sensing Committee which is chaired by of the National Geospatial-Intelligence Agency (NGA)

Multi-Process (tan)

1. Electronic Warfare (**EW**) process governs release of EW capability and technology based on inputs from multiple primary and secondary TSFD process owners under the leadership of OUSD(R&E), the National Security Agency (NSA), and OUSD(P) technical experts, including DTSA

Step 2 - Consultation and Engagement

Once the relevant TSFD pipes have been identified by the PMO, in consultation with their DoD Component IPO and local FDO, detailed engagement with each TSFD pipe owner should be pursued. Complex programs with leading edge DoD capabilities and technologies may require engagement with 5-10 different TSFD pipes. Moreover, each TSFD pipe owner requires that engagement efforts follow its policy and procedures including areas such as:

- Which DoD Component organization(s) are empowered to engage directly with the pipe (PMOs often must engage applicable pipes through an empowered organization within their DoD Component)
- The type of information required to obtain policy guidance/decisions from applicable pipes (While much of the program-specific information required by each pipe is similar, each pipe has its own format as well as unique information requirements it establishes)
- The way pipe decisions are made, documented, and recorded. (There is also a wide variance among the various pipes regarding their assessment methodology and criteria, decision documents, and recording of previous decisions that may establish relevant precedents for your program)

PMOs should be proactive within their DoD Component regarding TSFD pipe engagement activities. PMOs normally follow their DoD Component/FDOs lead regarding overall planning and engagement with pertinent TSFD pipes, but should also develop an internal PMO Plan of Action and Milestones (POA&M) (or equivalent) to ensure that all relevant TSFD pipe engagements are harmonized and synchronized with the program's Integrated Master Plan (IMP) and International Business Plan (IBP). The Defense Technology Security Administration (DTSA) International Engagement Directorate is also a resource available to PMOs, DoD Component IPOs, and FDOs seeking advice and insights regarding TSFD pipes pertinent to their program.

In addition to the USG/DoD TSFD process, PMOs should also be aware of USG Export Control considerations pertaining to their program. USG/DoD TSFD and USG export control review and approval systems are separate, but related. While obtaining USG export approvals are primarily a DoD contractor responsibility, PMOs are routinely asked by DoD Component IPOs and FDOs to provide program-specific advice on proposed USG export approvals under consideration by the State Department (for defense articles, services, and technical info on the U.S. Munitions List in the International Traffic in Arms Regulations (ITAR)) and the Commerce Department (for dual-use items and technology on the Commerce Control List (CCL) in the Export Administration Regulations (EAR)). Programs with substantial ICP involvement should consider developing a Defense Exportability Roadmap (see example template

prepared by DSMC-International faculty at Appendix A) to help integrate PMO and program contractor TSFD and export control -related activities.

PMOs and supporting personnel in various acquisition functional disciplines should participate, as applicable, in engaging the TSFD pipes, including the international manager, Systems Engineering (SE), and Systems Security Engineering (SSE) experts, the FDO, and the security manager. The PMO and functional organizations should work to ensure the government and contractor team TSFD, and export control-related efforts are aligned, harmonized, and synchronized. TSFD pipes and USG export license reviewers expect the PMO to perform this function. PMOs that employ this approach normally achieve desired TSFD and related export control approval outcomes. PMOs that do not employ this integrated approach encounter multiple problems and substantial delays in ICP, FMS, or hybrid FMS/DCS program formulation and execution.

While navigating the USG/DoD TSFD system, including navigation of each individual TSFD pipe relevant to a program, the PMO should understand that each TSFD pipe operates differently. PMOs should also recognize that each TSFD pipe must address potential dilemmas that arise while assessing U.S. national security, foreign policy, and operational demands to provide key capabilities to allies and friends against the potential risk of loss or compromise of key U.S warfighting capabilities and leading-edge technologies. PMOs, in consultation with their DoD Component IPO and FDO, should work closely with the relevant TSFD pipes in order to optimally balance competing USG/DoD objectives as an integral part of their efforts to establish a solid foundation for their program's current and future IA&E efforts.

C. Analysis & Evaluation -- Key Areas

PMOs, the international manager, and collaborating functional organizations should thoroughly address the following focal points when navigating the intricacies of TSFD as part of Defense Exportability Integration efforts:

1. Identification of Relevant TSFD Channels

- Has the PMO, in coordination with its DoD Component International Program Office (IPO) and Foreign Disclosure Officer (FDO), successfully identified all pertinent TSFD channels relevant to their IA&E efforts?

2. Engagement of Relevant TSFD Channels

- Has the PMO, working closely with its DoD Component IPO, FDO, and other essential TSFD-related entities, actively engaged all the pertinent TSFD channels?
- Has the PMO established a Plan of Action & Milestones (POA&M) or equivalent strategy to secure the necessary TSFD pipe policy guidance and approvals?

3. Export Control Plan for ICP-Centric Programs

- For programs with substantial ICP involvement, have the PMO and program contractor(s) developed an export control plan (see IA&E Guidebook Section 1-10) to help integrate PMO and program contractor TSFD and export control-related activities?

4. Effective Organization for TSFD Pipe Engagement

- Has the PMO structured itself effectively, with support from personnel in various acquisition disciplines, including an international manager, Systems Engineering (SE) experts, engineering professionals, Systems Security Engineering (SSE) experts, Foreign Disclosure Officer (FDO), security manager, and their counterparts among program contractors? (This coordinated approach is crucial to supporting successful TSFD pipe engagement activities.)

5. Balanced Pursuit of TSFD Pipe Outcomes

- Has the PMO maintained a consistent focus on achieving overarching TSFD pipe outcomes that strike an optimal balance between potential competing interests, including U.S. Government (USG) and Department of Defense (DoD) foreign policy objectives, operational requirements, and the protection of capability and technology for their program?

Section 4 – Exportability Design and Development

A. Foundational Building Blocks

As outlined in the preceding Sections of this JST, PMO exportability design and development efforts are based on two foundational building blocks – incorporation of system program protection measures and TSFD policy implementation through system differential capability modifications. PMOs, largely through their acquisition functional organizations, should focus on these two foundational building blocks in their program's exportability design and development efforts based on exportability objectives established in JCIDS ICDs/CDDs and/or the program's Acquisition Strategy (or equivalent documentation for agile acquisition efforts). The results of Program Protection (International Considerations) (Section 2) and Navigating the TSFD Pipes (Section 3) activities should be used to develop program-specific exportability requirements suitable for incorporation into program plans, international transaction mechanisms (.e.g., ICP international agreements, FMS cases, etc.), and associated contracting process documents. The IA&E Guidebook Section 1-4 provides overall guidance on the Defense Exportability Features (DEF) Program. Optimal exportability design and development solutions will enable the program to mitigate the potential risks as shown in Figure 3.

Figure 3: Domestic and International Exportability Design Considerations

Risks	Mitigations
Cyber-attacks (domestic and global) **Counterfeit Parts** (domestic and global supply chain) **Inadvertent Loss** (domestic or global) **Unauthorized Transfers** (by U.S. or foreign entities) **Foreign Espionage** (by U.S. adversaries, allies, and friendly nations (government & industry) **Foreign Exploitation** (by authorized or unauthorized system users, including equipment lost on the battlefield (US or export systems))	**Program Protection Measures** (the SSE, AT, Software Assurance, Hardware Assurance, Cybersecurity, and Supply Chain Risk Management, to include the use of Trusted Suppliers, used to protect U.S. and exportable systems) **TSFD Policy Decisions** (which define what may or may not be included in exportable systems from a capability and technology transfer perspective) **Differential Capability Modifications** (which remove unauthorized system capabilities and CPI, add unique customer nation requirements, and implement any other modifications required to achieve an exportable system configuration) **Information Security Measures** (the overall DoD CMI and CUI protection measures related to protection of all U.S. and exportable system information) **Physical Security** (use of "guns, gates, and guards" to protect U.S. and exportable version systems)

B. Feasibility Studies

PMOs should conduct DEF Feasibility Studies based on the detailed guidance contained in the USD(A&S) DEF Policy Guidelines as early as possible in the program's life cycle. DEF Feasibility Studies, which may be implemented through A&S's DEF Program or DoD Component Acquisition Executive (CAE)-approved Non-DEF Program arrangements, should be used to assess a system's defense exportability design trade space and define future DEF design and development efforts. The results of a program's initial DEF Feasibility Study should be used to:

- Establish the optimal number of exportable configurations of the system (Normally 2-4 different exportable configurations provide an optimal balance to achieve U.S. foreign policy, operational, and capability/technology protection objectives)
- Establish the detailed aspects of each exportable configuration with regard to differential capability and the "three pillars" of program protection (including anti-tamper) to mitigate potential risk of loss or compromise of key U.S warfighting capabilities and leading-edge technologies

The key challenges normally encountered in conducting an initial DEF Feasibility Study includes both the programmatic and technical aspects of exportability design. PMOs that have established and implemented a successful DEF Feasibility Study have been able to:

- Obtain early/timely DoD Component concurrence that an initial DEF Feasibility Study should be conducted by illustrating the potential magnitude (and benefits) of future phase ICP, FMS, DCS or BPC activity
- Engage program contractor(s) to convince them that conducting an initial DEF Feasibility Study would be advantageous from a U.S. industry (as well as USG) perspective
- Obtain funding to conduct an initial DEF Feasibility Study (*initial costs typically run in the $250K – $500K range)*
- Plan for follow-on funding to conduct actual DEF design efforts leading to development of one or more exportable system configurations either during the program's Engineering Manufacturing Development (EMD) phase or as part of a major program upgrade effort (*DEF design non-recurring costs can run anywhere from the low $M to substantially higher depending on various factors, but a mix of Title 10, DSCA Special Defense Acquisition Fund (SDAF), ICP, and/or FMS funding may be used to fund DEF design efforts)*

NOTE

The DEF Program funds activities to support identification of major defense acquisition programs for possible export and the planning for design and incorporation of exportability features during the research and development phases of these programs. Features include, but are not limited to, technology and engineering design activities such as capability differentials, anti-tamper, system assurance, and software assurance. Activities include the development of program protection strategies for the program; the design and incorporation of exportability features into the system; implementation of exportability requirements into contracts; and other research, development, test, and evaluation activities.

Key areas that may pose challenges in the actual conduct of initial DEF Feasibility Study and DEF design efforts include:

- Estimating future sales quantities of each exportable configuration(s) of the system
- Estimating non-recurring engineering (NRE) costs associated with designing and developing each exportable configuration of the system *(Note: the larger the number of exportable configurations, the higher the overall DEF NRE costs will be)*
- Finding and keeping government and contractor personnel with the specialized design skills (and associated security clearance requirements) needed to work effectively in AT, COMSEC, EW, and other highly classified design areas
- Projecting the potential threat environment 10-15 years into the future
- Employing a modular open systems architecture that will enable future TSFD-driven DC design changes to support product upgrades and an expanding sales market as the system matures

- Planning for future protection “technology refresh” design and development efforts to mitigate emerging risks

PMOs face the same types of challenges in designing for exportability as they do when designing and developing other demanding system characteristics. Due to the various uncertainties outlined above, PMOs normally find it difficult to achieve “perfect” exportability design outcomes during their program’s initial stages, but the old adage “best is the enemy of good enough” applies to DEF efforts as well. The PMO should conduct a “good enough” DEF Feasibility Study that implements an achievable set of exportability design features in its system exportable versions in order to achieve USG/DoD Security Cooperation engagement objectives while protecting leading edge DoD capabilities and technologies.

C. Analysis & Evaluation -- Key Areas

PMOs, along with the international manager and collaborating functional organizations, should carefully address the following pivotal considerations within their exportability design and development endeavors:

1. Exploration of Exportability Design via DEF Program

- Has the PMO initiated a DEF Program or DoD Component-approved DEF Feasibility Study to address key system program protection and TSFD policy considerations in order to explore potential exportability design efforts?

2. Optimal Number and Configuration Identification

- Based on the results of the DEF Feasibility Study, have the PMO and its functional personnel successfully determined the ideal number of exportable system versions and key specifications associated with each configuration?

3. Resolution of Programmatic and Technical Challenges

- Have the PMO and its functional experts effectively pinpointed, addressed, and resolved programmatic and technical hurdles that could impede future exportability design and development initiatives?

4. Contractor Support and Cost Sharing

- Are program contractors actively supporting exportability design efforts, and are they willing to invest in these initiatives upfront, notwithstanding the uncertainty surrounding cost recovery in the future?
- What strategies can the PMO employ to mitigate program contractors' apprehensions about government-industry cost sharing within the DEF Program?

5. Balanced Pursuit of Objectives

- Have the PMO and its functional specialists succeeded in establishing an exportability design and development strategy that harmoniously balances the often-competing objectives of USG and DoD foreign policy, operational requirements, and the safeguarding of capability and technology for their program?

Section 5 – International Security and Export Control

A. International Security Basics

International Security “basics” include an assessment of the allied or friendly nation’s willingness and ability to protect U.S. Classified Military Information (CMI) and Controlled Unclassified Information (CUI) as well as corresponding TSFD and export control-decisions regarding whether or not to grant access (see Section 3 of this JST for details). In accordance with DoD Directive 5230.11 “Disclosure of Classified Military Information to Foreign Governments and International Organizations”, and prior to any DoD

official's decision to grant access to CMI or CUI, the foreign government or private sector entity must agree in writing to:

- Not to transfer or use beyond authorized purposes without U.S. consent
- Provide substantially the same degree of security protection as the U.S.

B. Government-to-Government Transfers

PMOs should never transfer U.S. CMI or foreign government CMI under DoD's control unless they have verified the foreign government recipient has agreed in writing through an ICP Memorandum of Understanding (MOU), FMS Letter of Offer and Acceptance (LOA), or other USG/DoD approval document to provide such assurances pursuant to the applicable procedures in the U.S.- foreign government General Security Agreement (GSA) or equivalent. Policy and procedures for transfer of U.S CUI to foreign governments are in practice not as strict as those employed for CMI transfers since in most cases CUI is not governed by GSA procedures. However, PMOs are strongly encouraged to transfer U.S. CUI or foreign government CUI under DoD's control to foreign governments through pertinent ICP MOU, FMS LOA, Data/Information Exchange Annex, or other existing government-to-government mechanism. If none exists, consult your FDO or DoD Component IPO for guidance on how to arrange for the foreign government recipient to provide such assurances in writing prior to CUI transfer.

PMOs should never transfer U.S. CMI or foreign government CMI under DoD's control directly to foreign industry. CMI transfers to foreign industry must comply with the GSA procedures which require government-to-government involvement by the Designated Security Authorities (DSAs) of the U.S. and the foreign company's government. In general, PMOs should not transfer U.S. CUI or foreign government CUI directly to foreign industry. Instead, PMOs should transfer the CUI to the company's foreign government personnel responsible for managing ICP MOU or FMS LOA efforts and ask them to re-transmit the CUI to the foreign company.

C. Industry-to-Industry Transfers

PMOs should rely upon U.S. industry to obtain required USG and foreign export authorizations (see the next paragraph for details) prior to any industry-to-industry transfers of U.S. CMI and CUI. PMOs should never act as an agent or intermediary for transfer of U.S. CMI or CUI from U.S. industry to foreign industry without specific authorization from their FDO/DoD Component IPO.

D. Export Control Fundamentals

As a general rule, program contractors should obtain export authorizations from:

- Department of State (DoS) – for defense articles, services, and technical information on the U.S. Munitions List controlled by the International Traffic in Arms Regulations (ITAR)
- Department of Commerce (DoC) – for dual-use items and technology on the Commerce Control List (CCL) controlled by the Export Administration Regulations (EAR)

In certain circumstances, program contractors may be able to use ITAR exemptions rather than obtain export approvals from DoS. Since this is a complex area, PMOs should consult their FDO/DoD Component IPO to obtain specific advice regarding use of ITAR exemptions in support of their program's international acquisition activities. The EAR does not contain any provisions for exemptions and any required EAR export approvals must be obtained from DoC.

E. Export Control Considerations

In addition to PMO involvement in ITAR exemptions for program contractors, other PMO-related export control activities include:

- Working with program contractor(s) to contract for development and maintenance of an export control plan (see IA&E Guidebook Section 1-10) that helps synchronize separate but related

USG/DoD TSFD efforts and contractor-requested USG export approvals in support of the program's Integrated Master Plan (IMP) and International Business Plan (IBP).

- Facilitating DoS or DoC export approvals for export license requests through consultation and coordination with your FDO, DoD Component IPO, and the Defense Technology Security Administration (DTSA).
- Ensuring that PMO support contractors register with DoS as ITAR exporters to enable them to fully participate in ICP MOA/FMS LOA execution through DoS export license approvals or ITAR exemptions *(Note: This is an action that is often overlooked by PMOs.)*

NOTE

Per the DoDI 5000.85 and IA&E Guidebook, Section 1-4, programs with export markets must conduct an exportability roadmap study beginning no later than Milestone B. In the absence of a defined template within policy, DSMC-International faculty have created an example template in Appendix A of this JST.

F. International Security Arrangements

PMOs in consultation with their FDO/DoD Component IPO, local security organization(s), and their foreign security counterparts are responsible for establishing and implementing international security measures that are consistent with both national laws and security regulations/policies and the pertinent international arrangement (ICP MOU, FMS LOA, etc.). International security planning should be integrated with the program's overall security arrangements as early as possible. Key activities include:

- Identifying the projected number of foreign visits to program facilities in the U.S. and (if applicable) U.S. visits to foreign facilities
- Identifying U.S. facilities that will be routinely visited by foreign personnel, and ensuring that the local security organizations at these facilities are prepared to accommodate foreign personnel visiting (or working onsite) for program purposes
- Planning and executing ICP MOU Cooperative Program Personnel (CPP) or FMS LOA Foreign Liaison Officer (FLO) assignments in or near program facilities in accordance with DoD Directive 5230.20 "Visits and Assignments of Foreign Nationals", if applicable
- Establishing appropriate physical security and Information Technology (IT) access policies and procedures for CPPs, FLOs, and foreign visitors
- Providing applicable Delegation of Disclosure Authority Letter (DDL) guidance based on a need-to-know principle to U.S. personnel who will be working with foreign personnel at program facilities
- Developing and publishing PMO-level international security documentation including approval of an ICP MOU-required Program Security Instruction (PSI), if applicable prior to arrival of CPPs, FLOs, and foreign visitors at program facilities

Comprehensive and effective international security arrangements play an essential role in implementing USG/DoD program protection and TSFD and export control decisions. PMOs should work on a close and continuing basis with local FDOs and security organizations to provide day-to-day leadership and guidance to personnel across the entire spectrum of program activities to ensure that U.S. and foreign CMI and CUI is protected throughout the acquisition life cycle.

G. Analysis & Evaluation -- Key Areas

PMOs, in collaboration with the international manager and their respective functional organizations, should address the following critical considerations as part of international security and export control activities:

1. Training in International Security Fundamentals

- Have personnel within the PMO and supporting functional organizations undergone training in the fundamental principles of international security? This training should encompass guidelines for the proper handling, transmission, and safeguarding of U.S. CUI and CMI, as well as any CMI/CUI originating from foreign governments that may be in their possession.

2. Synchronization of TSFD and Contractor Export Control Efforts

- Has the PMO worked with program contractor(s) to plan and synchronize USG/DoD TSFD activities with contractor export control approval efforts that support ICP MOU and/or FMS LOA execution?

3. Integration of International Security Planning

- Has the PMO, in consultation with local FDOs and local security organizations, taken the necessary actions to integrate International Security planning and implementation with the program's overall security arrangements at the program facilities where DoD and foreign government/industry personnel will be working together or visiting?

Section 6 – Integration

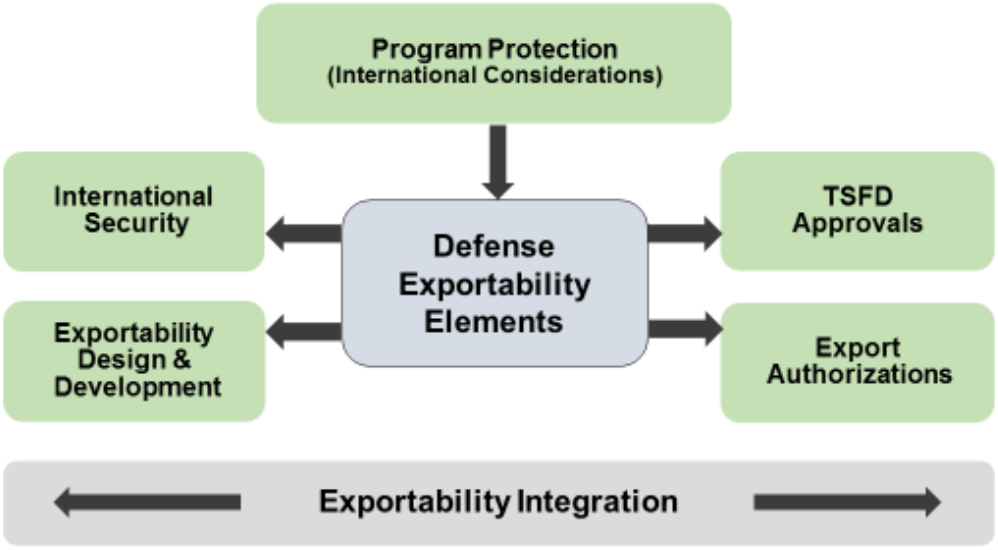
A. Conceptual Framework

PMOs should consider using the DEI Conceptual Framework (Figure 4) to help organize, plan, and integrate the various aspects of defense exportability within their programs.

PMO-level DEI efforts should initially focus on identification, design, development, and testing of exportability features that achieve DoD program protection requirements and comply with U.S. TSFD and Export Control policy decisions. Once this has been accomplished, PMOs should establish International Security measures, update U.S. TSFD decisions and exportable configurations, and work with industry on U.S. Export Control implementation matters, as appropriate, throughout the acquisition life cycle.

Effective PMO-level integration of program-level defense exportability efforts ensures that the PEO, DoD Component, OSD, Interagency, and Congressional levels are able to effectively review and if necessary, revise the program's exportability concept to ensure overall defense, foreign policy, and national security-level considerations are adequately addressed. DEI activities at the PMO level are complex, cross-cutting, and continuous,

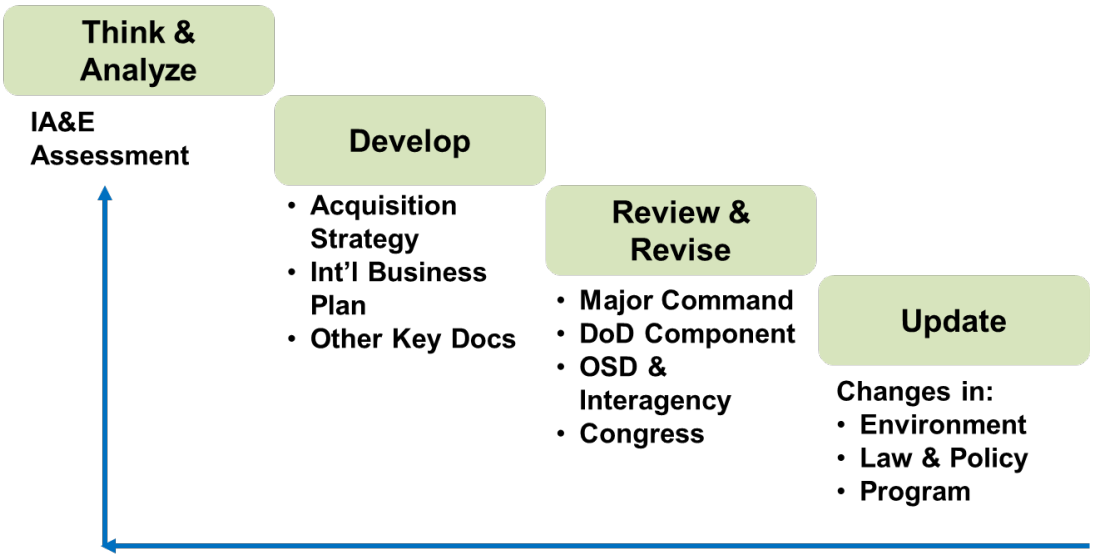
Figure 4: Defense Exportability Integration Conceptual Framework



B. Planning

PMOs should also consider using the Integration Planning Process depicted in Figure 5 to systematically assess each specific DEI area, develop harmonized DEI content in key planning documents (e.g., Acquisition Strategy, Program Protection Plan, etc.), evaluate proposed DEI-related revisions from higher levels, and maintain situation awareness regarding legal, policy, and programmatic changes that could affect the program's overall DEI implementation. Similar to other complex, interdependent acquisition efforts, the PMO's exportability integration efforts should attempt to rationalize and harmonize the activities of individual areas, guard against sub-optimized activities that detract from overall national security and foreign policy objectives and create a composite DEI approach that supports the program's desired international acquisition outcomes.

Figure 5: Defense Exportability Integration Planning Process

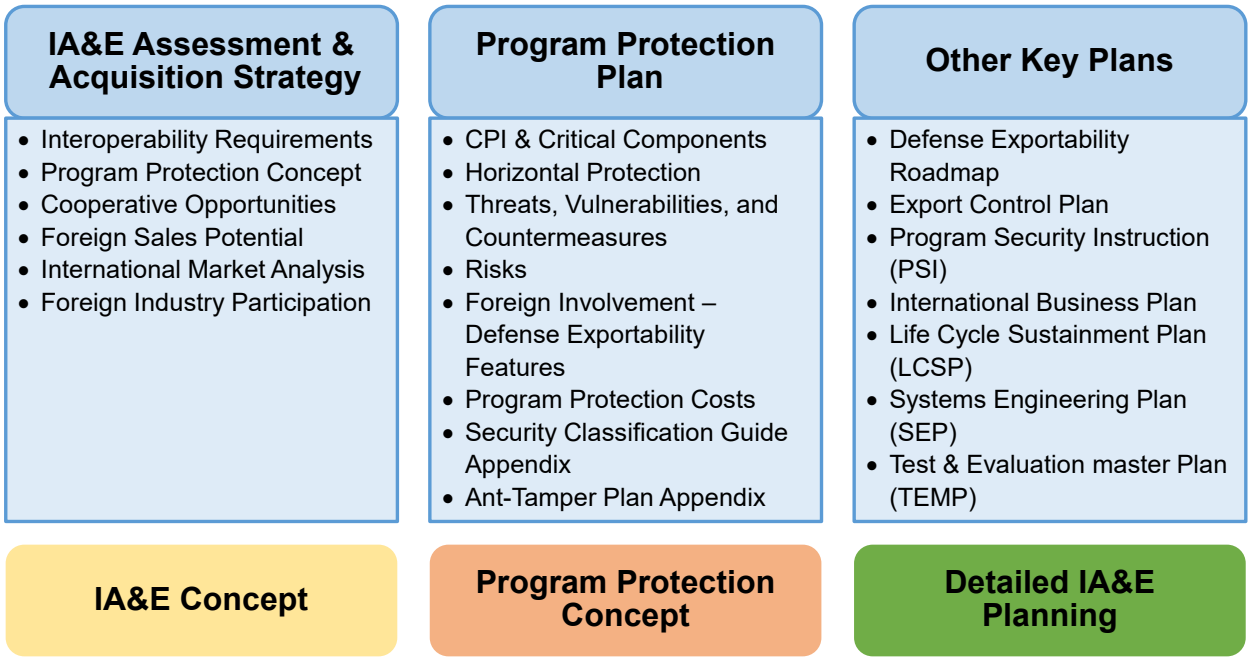


"The whole is much greater than the sum of the parts"

C. Documentation

The program's DEI approach should be incorporated in key program planning documentation beginning with the PMO's initial IA&E Assessment, through the Acquisition Strategy's international aspects and initial version Program Protection Plan, followed by detailed PMO-level planning (as applicable) in the specific functional areas as shown in Figure 6. PMOs should harmonize the DEI aspects of their various plans to ensure consistency, avoid gaps and seams at the conceptual and detailed levels, and establish an overall approach to exportability that helps achieve the program's international acquisition goals and objectives.

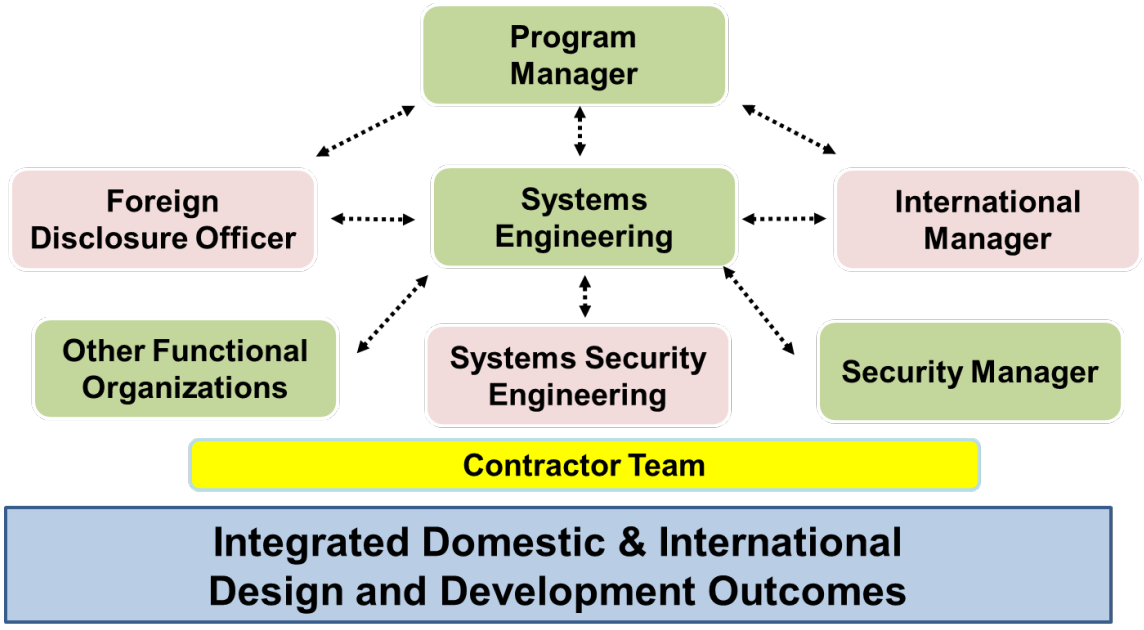
Figure 6: Defense Exportability Integration Documentation



D. Organization

PMOs and contractors that have integrated their domestic and international DEI efforts taking into account the organizational relationships shown in Figure 7 have been able to successfully pursue a wide variety of international acquisition efforts that provide DoD and the USG with mid-to-long term economic, political/military, and warfighting benefits. On the other hand, PMOs and contractors that organize and manage their DEI activities in a "stove piped" fashion often encounter many "do overs" in program protection, TSFD, DEF design and development, and export control activities. These "do overs" can drive unnecessary DoD indirect costs, extra PMO contractor work, lost foreign investment, lost economic order quantity benefits from foreign purchases, and higher direct costs to foreign ICP MOU partners and/or FMS customers. In extreme cases, such DEI inefficiencies result in lost foreign partnership or sale opportunities that not only hurt DoD economically, but have adverse national security, foreign policy, and operational effectiveness impacts. Effective DEI is a "team sport" that relies upon key contributions from a wide variety of PMO and functional personnel and their contractor team counterparts to achieve optimal domestic and international acquisition outcomes.

Figure 7: Defense Exportability Integration Organization



NOTE

While the systems engineer generally has a prominent role in DEI, Figure 7 does not portray all program office organizations or communication relationships. It is important to have cross-communication and collaboration across the team for successful design and development integration outcomes.

E. Challenges and Solutions

DEI efforts at the PMO level can pose many challenges as shown in Figure 8. This is an unpleasant fact that all programs with substantial international acquisition involvement have had to eventually face in the acquisition life cycle. PMOs may feel that it's unreasonable that they have to bear such a substantial part of the burden of DEI implementation when many of its aspects, especially the establishment and maturation of political/military relationships with foreign nations, formulation of TSFD policy guidance, and export control decision making lie outside of the DoD acquisition community's span of control.

The middle column in Figure 8 highlights many of the typical shortcomings that PMOs encounter if they decide: 1) not to pursue an integrated DEI approach early in the program; or, 2) manage the program's domestic and international DEI efforts in completely separate stovepipes. These challenges have been routinely observed over the years in DoD acquisition programs with substantial international involvement, especially affected by external forces such as USG political/military relationships, USG/DoD security cooperation objectives, Combatant Command operational requirements, and domestic and global industrial forces. On the bright side, PMOs that face these challenges early and organize their domestic and international DEI efforts to meet them using the best practice suggestions in Figure 8's right hand column put themselves (and their successors) in a position to achieve USG/DoD desired political/military and operational results as well as program stability and economic benefits in future years.

Figure 8: Defense Exportability Integration Challenges and Solutions

Area	Typical Shortcomings	Best Practice Solutions
TSFD	▪ Missed TSFD pipes ▪ Conflicting/confusing pipe policy ▪ Costly/technically infeasible policies	▪ Seek expert TSFD advice early on ▪ Engage proactively with pipes ▪ Provide facts and realistic options
DEF	▪ Higher authority doesn't support ▪ Insufficient funding ▪ TSFD pipe guidance lacking	▪ Justify in Milestone Decision process ▪ Pursue various funding sources ▪ Early engagement with TSFD experts
Int'l Security	▪ Domestic/int'l security separated ▪ Facility/IT Sec Mgrs not engaged ▪ Functional disciplines not engaged	▪ Use integrated security approach ▪ Involve Facility/IT Sec Mgrs early on ▪ Ensure functionals participate
Export Control	▪ Industry unaware of TSFD policy ▪ Industry ignores TSFD policy ▪ TRR not contractually required	▪ Share TSFD policy with industry ▪ Use EC process to control industry ▪ TRR made contract deliverable
Integration	▪ One or more key areas ignored ▪ Parts are managed, whole is not ▪ Lack of leadership & organization	▪ Systematic PP planning and updates ▪ Develop PP Teamwork processes ▪ Int'l Mgr/FDO lead integration efforts

F. Analysis & Evaluation -- Key Areas

PMOs, working closely with the international manager and supporting functional organizations, should examine the following key considerations as part of the program's integration activities:

1. Consideration of Future Defense Exportability

- Has the PMO sufficiently contemplated the prospect of future defense exportability throughout the program's MSA, TMRR, and EMD phases?

2. Comprehensive Integration of DEI Considerations

- Has the PMO methodically integrated and consistently updated DEI considerations within the program's Acquisition Strategy, Program Protection Plan, and other critical program plans?

3. Analysis of Three Pillars of Program Protection

- Have the PMO and its functional experts conducted a thorough analysis of the three pillars of program protection - Information, CPI, and TSN - to discern what requires protection, both within the domestic and international contexts?

4. Identification of Relevant TSFD Pipes

- Has the PMO identified the specific TSFD pipes that are pertinent to the international aspects of the program?
- Has an action plan been devised to secure the requisite TSFD approvals?

5. Conducting Initial DEF Feasibility Study

- Has the PMO established arrangements with program contractor(s) to undertake an initial DEF Feasibility Study?

6. Optimal Exportable Configurations Determination

- Has the DEF Feasibility Study identified the ideal set of exportable configurations, considering both number and capability, based on guidance from TSFD pips and program protection considerations?
- Have Differential Capability (DC) and Anti-tamper (AT) aspects been determined for each exportable configuration?

7. Cost-Benefit Analysis for Exportability Design and Development

- Have the PMO and its Systems Engineering (SE) and Systems Security Engineering (SSE) experts established a process for conducting cost-versus-benefit trade-off analyses concerning exportability design and development alternatives in terms of DC and AT?

8. Establishment of International Security Policies

- Are PMO-level international security policies and procedures in place?
- Are domestic and international security considerations integrated across all program facilities?

9. Inclusion of Export Control Plan in Contracts

- Have the PMO and program contractor(s) incorporated an export control plan into relevant contracts to facilitate tracking and alignment of government and industry TSFD pipe approvals and export control authorization activities?

10. Integration of Program Protection Measures

- Have the PMO and its functional experts effectively integrated program protection, TSFD, DEF, international security, and export control measures across all international acquisition domains (ICP, FMS, DCS, BPC, and International Contracting) to ensure robust protection of Information, CPI, and TSNs?

11. Proactive Use of DEI Best Practices

- Has the PMO and its functional personnel been proactive in implementing best practices in Defense Exportability Integration (DEI) throughout the program's life cycle?
- Are these practices aligned with current and future USG/DoD political, military, and operational objectives, as well as program stability and economic benefits?

Glossary

In addition to the DAU Glossary, which is a useful resource, the following list of key terms is provided to assist DEI JST users:

ACRONYM	ACRONYM SPELLED OUT
AAF	Adaptive Acquisition Framework
AT	Anti-tamper
ATEA	Anti-Tamper Executive Agent
BPC	Building Partnership Capacity
CAE	Component Acquisition Executive
CDD	Capabilities Development Document
CIO	Chief Information Officer
COMSEC	Communications Security
CPI/CC	Critical Program Information/Critical Components
CPP	Cooperative Program Personnel
CMI	Classified Military Information
CUI	Controlled Unclassified Information
DC	Differential Capabilities
DCS	Direct Commercial Sales
DCSA	Defense Counterintelligence and Security Agency
DDL	Delegated Disclosure Letter
DEF	Defense Exportability Features
DEI	Defense Exportability Integration
DL/WF	Data Link/Waveform
EC	Export Control
EMD	Engineering and Manufacturing Development
EW	Electronic Warfare
FDO	Foreign Disclosure Officer
FLO	Foreign Liaison Officer
FMS	Foreign Military Sales
GEOINT	Geospatial Intelligence
IA&E	International Acquisition and Exportability
IBP	International Business Plan
ICD	Initial Capabilities Document
ICP	International Cooperative Program
ICT	Information and Communications Technology
ITAR	International Traffic in Arms Regulation
JCIDS	Joint Capabilities Integration and Development System
JST	Job Support Tool
JROC	Joint Requirements Oversight Council
LO/CLO	Low Observable and Counter Low Observable
LOA	Letter of Offer and Acceptance
MCA	Major Capability Acquisition
MIDP	Military Intelligence Disclosure Policy
MOU	Memorandum of Understanding
MSA	Materiel Solution Analysis
MTA	Middle-Tier Acquisition
MTCR	Missile Technology Control Regime
NDP	National Disclosure Policy
NSA	National Security Agency
NVD	Night Vision Device
PMO	Program (or Project) Management Office
PNT	Positioning, Navigation, and Timing

PPP	Program Protection Plan
PSI	Program Security Instruction
S&T	Science & Technology
SE	Systems Engineering
SSE	Systems Security Engineering
TAPP	Technology Area Protection Plan
TMRR	Technology Maturation and Risk Reduction
TSFD	Technology Security & Foreign Disclosure
TSN	Trusted Systems and Networks

Note: If you would like to provide feedback on this JST, have ideas for improvement, have questions on this JST, or would like advice on how to use this JST in the workplace, please send an email to InternationalHelp@dau.edu.

Program International Acquisition & Exportability (IA&E)

Exportability Roadmap Template[1]

I. Introduction

Briefly describe the context/events that led the PM, PEO, and/or Milestone Decision Authority (MDA) to decide to incorporate the Defense Exportability Features (DEF) into the system needed to make future defense sales. Summarize and incorporate by reference any key program decision documents (e.g., Acquisition Strategy, Milestone Decision Document(s), etc.) that are pertinent.

a. **Program Protection Overview:** Provide a CUI-level summary of the program's DEF-related Program Protection Plan (PPP) aspects. If no PPP exists, develop a CUI-level summary in consultation with the program's System Engineer, System Security Engineer, and FDO.
b. **TSFD Overview:** Provide a CUI-level summary of any existing or 'in-process' DoD Component, DoD, or USG Technology Security Foreign Disclosure (TSFD) assessments or guidance pertinent to the program's DEF efforts. Reference any pertinent classified written or oral TSFD guidance. Consult with your local Foreign Disclosure Officer (FDO), if needed.

II. Potential Foreign Sales/Transfers

The PM/IPT – with assistance from their DoD Component International Programs Organization (IPO), program contractor(s), and other key stakeholders -- develop a realistic estimate of potential/projected foreign sales or transfers of the system, including the relative interest in the system, timing, and projected level of sales. Include both qualitative and quantitative aspects your analysis and results since these will be needed to complete Section IV (DEF Differential Capabilities) and Section V (Business Case Analysis).

III. Holistic Program Protection Measures (PPMs)

If not already accomplished/defined in the system's PPP, the PM/IPT must analyze the U.S. version system's leading edge warfighting capabilities & technologies that require PPMs in the following areas:

a. **Communications Security (COMSEC)** – that requires use of National Security Systems (NSS) to protect Classified Military Information (CMI) and Controlled Unclassified Information (CMI) C3 radio and data link transmissions.
b. **Cyber** – that requires use of various cybersecurity measure to protect CUI in the system, product support system, acquisition program management, and government/industry program infrastructure.
c. **Critical Program Information (CPI) and Critical Technologies (CT)** – that requires use of Anti-Tamper (AT) measures in program-specific and 'legacy' GFE/X hardware, firmware, and software.
d. **Product Support & Supply Chain Risk Management (SCRM)** – that requires use of Trusted Systems & Networks (TSN) protective measures in the program's life cycle logistics infrastructure.

[1] Consult the DAU Defense Exportability Integration (DEI) Job Support Tool (JST) -- URL https://www.dau.edu/tools/defense-exportability-integration-job-support-tool-jst -- as needed, during PM/IPT Exportability Roadmap development efforts.

The PM/IPT should identify technical feasibility and non-recurring engineering (NRE) costs projected for completing a U.S. version system design that meets the "one size fits all" program protection for both domestic and exportable system configurations. This effort should include analysis of:

e. **PPM Technical Feasibility and NRE Costs** - associated with developing 'one size fits all' program protection measures and conducting developmental testing & evaluation (DT&E) activities per DODI 5000.89 (Test & Evaluation) on components and software that require PPMs for domestic system configuration(s) as well as exportable system configuration(s).
f. **DoD Funding Requirements** – associated with design and develop the "one size fits all" PPMs defined by the analysis effort described in subparagraph III d. above since these program protection requirements are a DoD Title 10 responsibility and should be funded by DoD RDT&E Program Elements (PEs)

IV. DEF Differential Capabilities (DC)

The PM/IPT should also evaluate the program's design architecture approach to determine whether Modular Open Systems Architecture (MOSA) standards/approach will or won't be used in the system, then analyze DC areas (and associated DC configuration change requirements) that will need to be addressed based on DoD Component and DoD/USG TSFD "pipe" policy guidance that pertains to the system.

Alternative 1

a. **TSFD Guidance**: The PM/IPT will need to engage with DoD Component and local FDO personnel to identify and define DoD Component (e.g., Navy Tech Transfer & Security Assistance Review Board (TTSARB), Air Force Top-line process, and DoD/USG TSFD "pipe" policy (e.g., NDPC, LO/CLO, CNSS/CJCSI 6510/GPS/Data Link/WF) guidance).[2]
b. **DC Requirements Definition**: If a MOSA standards/approach (funded by DoD RDT&E PE(s) since this is a DoD requirement) is being used during system development, the PM/IPT will need to identify the export configuration-specific technical feasibility and NRE costs associated with incorporating any TSFD-driven Differential Capability (DC) requirements. This typically results in the PM/IPT defining one or more Exportable Configurations, taking into account the program's Defense Exportability Integration (DEI) strategy with respect to Best Friends (BF), Good Friends (GF), Friends (F) and Acquaintances (A) based on the potential defense sales/transfers identified in Part II (Foreign Sales/Transfers Analysis).
c. **DC NRE Cost Estimating**: Next, the PM/IPT should develop a MOSA-based NRE cost estimate for each Exportable Configuration that the PM, PEO, and MDA decide are needed (e.g., two Exportable Configurations, one for BFs/GFs and one for Fs/As).
d. **DC Feasibility Assessment:** The final step is PM/IPT assessment of the feasibility of obtaining foreign partner/customer funding to design and develop at least one MOSA-based Exportable Configuration (e.g., BF/GF) defined by the analysis efforts described in subparagraphs IV b. & c. above since the actual DC NRE costs for each Exportable Configuration must be funded by Int'l Cooperative Program (ICP) partner nations and/or FMS customer nations (DoD funding cannot be used for this purpose unless it is specifically authorized/appropriated by Congress).

[2] Consult DEI JST Section 3.

Alternative 2

e. **TSFD Guidance**: The PM/IPT use the same approach as Alternative 1.
f. **DC Requirements Definition**: If a MOSA standards/approach was not/is not being used during system development, the PM/IPT will still need to identify the export configuration-specific technical feasibility and NRE costs associated with incorporating any TSFD-driven DC requirements. This also typically results in the PM/IPT defining one or more Exportable Configurations, taking into account the program's DEI strategy with respect to potential defense sales/transfers to BF/GF/F/A countries identified in Part II (Foreign Sales/Transfers Analysis). However, the technical challenges -- and corresponding NRE costs associated with DC-required configuration mods -- tend to be much greater.
g. **DC NRE Cost Estimating**: Next, the PM/IPT will need to develop a non-MOSA-based NRE cost estimate for each Exportable Configuration that the PM, PEO, and MDA decide are needed.
h. **DC Feasibility Assessment:** Finally, the PM/IPT will need to assess the feasibility of obtaining foreign partner/customer funding – usually a much higher amount than Alternative 1 -- to design and develop at least one MOSA-based Exportable Configuration (e.g., BF/GF) defined by the analysis efforts described in subparagraphs IV b. & c. above since the actual DC NRE costs for each Exportable Configuration must be funded by Int'l Cooperative Program (ICP) partner nations and/or FMS customer nations (DoD funding cannot be used for this purpose unless it is specifically authorized/appropriated by Congress).

V. Business Case Analysis (BCA)

The PM/IPT should conduct a defense exportability BCA that compares the anticipated program DEF PPM and DC resource demands and investment costs for the development of one or more Export Configurations against the potential Return on Investment (ROI) from anticipated foreign ICP investment in and/or FMS, DCS, or FMS/DCS hybrid procurement of the system.

a. **Qualitative**: The qualitative aspect of the BCA should evaluate the breadth and depth of potential USG/DoD benefits in operational coalition warfare capability/interoperability and establishment/expansion of political-military relationships vis-à-vis the allied/friendly nations identified in Part II that are likely to acquire the system due to incorporation of affordable DEF.
b**. Quantitative**: The quantitative aspect of the BCA should assess and calculate the PM/IPT resource demands and up-front DoD NRE investment costs -- primarily in "one size fits all" PPMs (Part III) and MOSA to facilitate DEF DC incorporation (Part IV) – that will most likely achieve U.S. ICP, FMS, DCS, or Hybrid sales 'targets' established in Part II.
c. **Trade-Off Analysis**: Most DEF BCAs include a 'trade-off' section – which includes sensitivity analysis of both qualitative and quantitative assessments and values – focusing on the following key variables:

1) ***Optimal Number of Exportable Configurations***: One Exportable Configuration (e.g., BF only) is the least expensive to design and develop but may not achieve desired system sales targets. Four Exportable Configurations (BF, GF, F, A) may result in achievement of desire system sales targets but would place too many demands on PM/IPT and program contractor(s) and be unaffordable.
2) ***Optimal PPM Approach***: Most PMs/IPTs will have to use a Risk, Issue, and Opportunity (RIO) Management approach to define a holistic mix of PPMs that adequately address the risks of system

compromise -- taking into account the technical feasibility and affordability of specific PPMs in each major PPM (Cyber, COMSEC, AT, TSN) – that are programmatically achievable and affordable.[3]
3) ***Optimal DC Approach***: Most PMs/IPTs will also have to use an RIO-like approach in their engagement with the TSFD 'pipe owners' that adequately address the risks of system export -- taking into account the technical feasibility and affordability of DC modification requirements generated by the TSFD Pipes – to ensure that TSFD Pipe guidance is programmatically achievable and affordable.

VI. RECOMMENDED DEF COURSE OF ACTION (COA)

The PM/IPT should develop a recommended DEF COA for PEO and MDA approval that addresses:

a. **Number of Exportable Configurations**: Recommend a programmatic/technically feasible and affordable number of exportable variants of the system, such as: export to BFs only; export to BFs/GFs that are proven coalition partners; export to a wide range of allied and friendly nations (including Fs/As) around the world.
b. **PPMs & TSFD Requirements**: Recommend programmatic/technically feasible PPMs and DC modifications that correspond with the recommended Export Configurations in paragraph VI a. that address DoD program protection policy and USG/DoD TSFD policy guidance pertaining to the system.
c. **COA Summary**: The requirements, performance, cost, and schedule aspects of each Exportable Configuration should be summarized to establish a baseline for oversight, management, and future evaluation of the program's recommended DEF efforts.

See following example:

BF/GF Exportable Configuration

Performance:

PPMs: "One size fits all" DoD-funded PPMs address all program protection requirements except for DC modification #2 that will require additional DEF PPM design & development (D&D).

DC: Four DEF DC D&D modifications are required by TSFD Pipe policy (provide CUI descriptions with references to Classified TSFD policies) – DC #1 (Hardware (HW) and Software (SW); DC #2 (HW & SW); DC #3 (HW); DC #4 (SW).

Cost Estimate(s) and Funding Source(s):

DEF Mod #	DEF Mod Description	D&D NRE Cost Estimate	Funding Source
PPM #1	Driven by DC#2	$0.xxK	ICP with **BFs** A & B
DC #1	HW … and SW …	$X.xxK	" "
DC #2	HW … and SW …	$X.xxK	" "
DC #3	HW …	$X.xxK	" "
DC #4	SW	$0.xxK	" "

BF/GF Exportable Configuration (cont.)

Schedule:

[3] DoD Risk, Issue, and Opportunity Management Guide for DoD Acquisition Programs, URL https://www.dau.edu/tools/risk-and-opportunity-rio-guide

PPMs: Develop Program Plan schedule chart showing all key D&D events (including T&E and 'approval')

DC: Develop Program Plan schedule chart (including T&E and 'approval')

F/A Exportable Configuration

Performance:

PPMs: "One size fits all" DoD-funded PPMs and BF/GF PPM #1 address all program protection requirements except for DC modification #6 that will require additional PPM DEF design & development (D&D).

DC: Two additional DC configuration D&D modifications are required by TSFD Pipe policy beyond BF/GF DC mods (provide CUI descriptions with references to Classified TSFD policies) – DC #5 (HW & SW); DC #6 (SW).

Cost Estimate(s) and Funding Source(s):

DEF Mod #	DEF Mod Description	D&D NRE Cost Estimate	Funding Source
PPM #2	Driven by DC#6	$0.xxK	FMS 'Launch Sale' LOAs with **Fs** C & D
DC #5	HW … and SW …	$X.xxK	" "
DC #6	SW …	$0.xxK	" "

Schedule:

F/A Exportable Configuration development will begin after BF/GF configuration development has reached its T&E phase.

PPMs: Develop Program Plan schedule chart showing all key D&D events (including T&E and 'approval')

DC: Develop Program Plan schedule chart (including T&E and 'approval')

VII. DEF Implementation

The PM/IPT should describe the approach they will use to ensure that approved DEF COA design and development requirements for each approved Exportable Configuration are integrated/included in the overall Program Master Plan (or equivalent), Systems Engineering Plan, Program Protection Plan, and Life-Cycle Sustainment Plan.