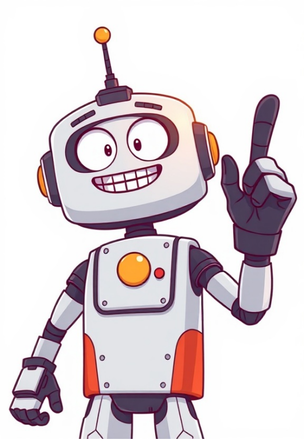
Continue



AT measures are implemented to safeguard Critical Program Information (CPI) in US defense systems developed with co-development agreements or sold to foreign governments; these measures aim to prevent exploitation and delay countermeasure development. ==========The US Department of Defense has issued a new guidance document that outlines measures for protecting sensitive technologies in weapon systems from unauthorized access or tampering. ========== This guidance applies to various aspects of US defense programs, including system performance, materials, hardware, software, and design methods. The DoD 5000 series will include provisions for incorporating Anti-Tamper (AT) into acquisition programs. While AT is a protective measure, it should not be seen as a substitute for physical security protocols. ATTENTION TO DETAIL IS KEY Program Managers are required to involve all relevant stakeholders in the inclusion of AT in their programs, including Service, Defense Agency, and OSD comptrollers, financial management organizations, and users. Funding decisions must be based on thorough risk analysis and proper justification. INTERNATIONAL COOPERATION IS KEY TO SUCCESS The DoD actively seeks cooperation with foreign allies and partners to develop and acquire weapon systems. This cooperation can lead to shared development costs, reduced production costs, and strengthened domestic industrial bases. However, the US government must also ensure that sensitive technologies are protected from unauthorized access or tampering. TECHNOLOGY IS TODAY'S FORCE MULTIPLIER The use of sophisticated technology in defense systems is crucial for their effectiveness on the battlefield. Protecting critical technologies is essential to preserving the US government's resources and technological investment. ========== In order to boost US competitiveness in the global market, investments in R&D should be viewed as a financial outlay rather than an expenditure. One method used to safeguard critical weapon system technologies is by employing Anti-Tamper techniques and technology. ## Discussion: 1. Anti-Tamper involves a comprehensive approach to protecting sensitive technologies throughout the entire systems development lifecycle. This includes conducting thorough research, design, testing, and implementation of Anti-Tamper measures. 2. The aim of Anti-Tamper is not to completely thwart exploitation but rather to deter it by making the process as time-consuming and costly as possible. This should enable the US and its allies sufficient time to develop new technologies, thereby safeguarding their military capabilities. ## Discussion: 3. Anti-Tamper is closely linked with Program Protection Plans (PPP) outlined in reference B (DoD Dir 5200.39). The AT annex will be integrated into each PPP as an additional layer of protection. 4. Depending on the technologies involved, some acquisition programs may not require a PPP or AT measures. However, a thorough evaluation is necessary to determine whether such protections are needed. 5. The Defense Acquisition Deskbook and DoD 5000 series will provide guidance on PPP and AT annexes in future revisions. ## Discussion: 6. The level of protection required for each program depends on the sensitivity of its technologies. Evaluations can be conducted by independent third-party experts, including US Government laboratories or contractors without conflicts of interest. 7. The Militarily Critical Technologies List (MCTL) is an essential resource for assessing technology sensitivity. Program Managers should consult this list to determine whether their planned technologies are included. ## Discussion: 8. OUSD(AT&L) oversees Anti-Tamper issues and provides guidance to PMs as part of its program oversight responsibilities. 9. The Defense Technology Analysis Office offers advice, assistance, and access to AT-capable organizations for Program Managers. ## Guidelines for Anti-Tamper Disclosure: 10. Information regarding the implementation of AT measures should only be unclassified if the Component and MDA have deemed it suitable for disclosure. 11. Techniques and methods used in implementing AT may be classified up to SAP levels as necessary, and any non-US entities or individuals will not be informed about such classified information pursuant to established disclosure channels. ==========The program's MDA shall coordinate all foreign disclosure releases involving AT with the cognizant foreign disclosure office and security assistance office as approprate. An Exception to National Disclosure Policy may be warranted for co-development programs, Foreign Military Sales, or Direct Commercial Sales.G. -- Implementation:1. AT is a systems engineering activity that must be initiatied in program definition and risk reduction. AT is applicable to P3I upgrades or other technology insertion to fielded systems. AT requires resources and thus may affect other aspects of the program to include the cost and performance of the end product. AT involves risk analysis, and the decision not to implement AT must be based on operational risks involved as well as on acquisition risks including, but not limited to, feasibility, cost, system performance impacts, and schedule impacts.2. AT shall be included in requirements development for all new acquisition programs effective with this memorandum. AT shall not be required for fielded systems or those that have passed Milestone II, because AT may be difficult or impossible to retrofit. However, AT shall be considered in any product improvement engineering effort for these systems. The use of AT may be required for programs, regardless of their acquisition status, at the discretion of the MDA.3. AT shall be considered for use on any conventional system developed with allied partners, likely to be sold or provided to U.S. allies and friendly foreign governments, or likely to fall into enemy hands. If the system is not likely to be exposed to these scenarios, then AT may not be required. This decision, however, must be deliberate, fully supported, and documented in the PPP's AT annex.4. U.S. weapon systems not intended for foreign distribution through FMS, DCS, or other avenues but that may fall into enemy hands on the battlefield shall include AT if critical technologies are involved.5. The decision to use or not to use AT will be documented in a classified annex to the Program Protection Plan. The PM should consider using a qualified disinterested party to conduct the technology assessment and advise whether implementation of AT is required. The disinterested party may be a Federally Funded Research and Development Center, a contractor that is free from conflict of interest, a university, or another Federal government agency. The Prime contractor may be used only if a qualified disinterested third party cannot be used.6. If AT is determined necessary, the AT classified annex to the PPP will contain AT planning. The planning detail will correspond to the phase of the development of the program. The AT annex should also include, but is not limited to, the following information: identification of the critical technology being protected; how long AT is intended to delay hostile exploitation or reverse-engineering efforts; description of the planned AT approach; the effect compromise would have on the acquisition program if AT is not implemented; the estimated time and cost required for system or component redesign if compromise occurs; and the program's AT point of contact. The AT annex to the Program Protection Plan will be developed for Milestone II and updated at subsequent milestones.7. AT applicability will be assessed for each major modification or P3I upgrade to the production system. It is feasible that AT may be inserted into the modified or upgraded systems if protection is required, or that AT may be discontinued when it is assessed that the technology no longer needs to be protected.8. The recommendation to implement or not to implement AT will be approved by the responsible MDA. OUSD(AT&L) will keep abreast of AT as part of its program oversight role.9. Service Acquisition Executives and OUSD(AT&L) shall be kept apprised of the status of AT in any program, including AT implemented in a SAP. Personnel in these offices shall be granted access to the SAP program in order to perform oversight functions should AT be implemented in a SAP program or should the AT itself require a SAP.10. AT, whether implemented or not, will be a discussion item at Milestone II and Milestone III decision points. At Milestone II, AT shall be addressed in conceptual terms of how it is to be implemented; working prototypesTo demonstrate this stage of program development, the Milestone III decision shall not be given favorable consideration until actual implementation is fully documented, tested during Development Test (DT) and Operational Test (OT), and ready for production. ==========___ Deliverables at Milestone II will include: * A list of critical technologies * A threat analysis * Identified vulnerabilities * And a preliminary Anti-Tamper (AT) requirement Deliverables at Milestone III will include: * All deliverables from Milestone II and any updates * An analysis of AT methods that apply to the system, including cost/benefit assessments * An explanation of which AT method(s) will be implemented * A plan for verifying and validating the AT implementation These deliverables will be submitted as part of the AT annex to the Public Private Partnership (PPP). ==========___ AT shall be verified and validated after weapon system implementation. This task shall be performed by a third party on actual or representative system components. The Verification and Validation (V&V) plan shall be reviewed at Milestone III. The V&V plan results shall be reported to the appropriate Service Acquisition Executive and OUSD(AT&L). ==========___ AT shall not be limited to developing and fielding a system. Equally important is life cycle management, particularly maintenance. Maintenance instructions and technical orders must clearly indicate that AT techniques have been implemented, the level at which maintenance is authorized, and warnings that damage may occur if improper or unauthorized maintenance is attempted. It may be necessary to limit the level and extent of maintenance a foreign customer may perform in order to protect critical technologies. This may mean that the level of maintenance that involves the AT will be accomplished only at the contractor or U.S. Government facility in the United States or overseas. Such maintenance restrictions must be stated in the appropriate contracts, PA, MOU, MOA, LOA, or other similar documents. The U.S. Government and U.S. industry must be protected against warranty and performance claims in the event AT measures are activated by unauthorized maintenance or other intrusion. Such unauthorized activities shall be regarded as hostile attempts to exploit or reverse engineer the weapon system or the AT technique itself and shall void warranties and performance guarantees. ==========___ Figure 1 is a representation of a generic decision process for implementing AT in a program. To fully support the systems engineering approach that defines the AT concept, participation of the acquisition program's Overarching Integrated Product Team (OIPT) is strongly recommended. The Director, Strategic and Tactical Systems, will convene a standing OIPT to oversee and guide the use of AT in DoD acquisition programs and build a centralized AT technologies resource reference database for use by the acquisition community.The Department of Defense's Foreign Military Sales (FMS) Program is a crucial mechanism for the acquisition of defense-related articles and services from foreign countries. The FMS Program allows the U.S. government to sell military equipment and technology to allies and partners in exchange for economic and strategic benefits. # Letter of Offer and Acceptance A Letter of Offer and Acceptance (LOA) is a critical document that outlines the terms and conditions of the sale, including the type and quantity of items to be delivered, payment terms, and any other relevant details. The LOA serves as the foundation for the entire FMS transaction. # Milestone Decision Authority Milestone Decision Authority (MDA) refers to the process by which critical decisions are made during the acquisition process. MDA ensures that key milestones are met, such as the completion of design and development activities or the delivery of major components. # Memorandum of Agreement (MOA) A Memorandum of Agreement (MOA) is a non-binding document that outlines the general terms and conditions of the FMS transaction. The MOA provides a framework for negotiations and serves as a precursor to the LOA. # Memorandum of Understanding (MOU) A Memorandum of Understanding (MOU) is a high-level agreement that establishes the scope and objectives of the FMS transaction. The MOU provides a general outline of the terms and conditions, but it is not binding like an LOA. # Overarching Integrated Product Team The Overarching Integrated Product Team (OIPT) is a collaborative effort between various stakeholders to ensure that defense-related articles and services meet U.S. government requirements. The OIPT brings together experts from multiple agencies and industry partners to develop and deliver complex systems. # Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) plays a critical role in overseeing the FMS Program. The office is responsible for developing and implementing acquisition strategies, managing budgets, and ensuring that defense-related articles and services meet U.S. government requirements. # Project Arrangement A Project Arrangement is a contract that outlines the terms and conditions of the FMS transaction. The arrangement typically includes provisions related to payment, delivery, and support. # Pre-Planned Product Improvement Pre-Planned Product Improvement (P3I) refers to the process by which defense-related articles and services are improved or upgraded before they are delivered to foreign governments. P3I enhances the performance and capabilities of these systems, ensuring that they meet U.S. government requirements. # Program Executive Officer The Program Executive Officer (PEO) is responsible for overseeing specific defense programs and initiatives. The PEO works closely with stakeholders to ensure that projects are completed on time and within budget. # Program Manager A Program Manager is a critical professional who leads the development and implementation of defense-related articles and services. The program manager ensures that projects meet U.S. government requirements and are delivered in accordance with established schedules and budgets. # Program Protection Plan (PPP) The Program Protection Plan (PPP) is a document that outlines the measures taken to protect defense-related articles and services from unauthorized disclosure or use. The PPP ensures that sensitive information remains confidential, even after delivery of these systems. # Special Access Program A Special Access Program (SAP) refers to defense-related articles and services that require special access controls due to their sensitivity. SAPs are used for the development and testing of new technologies, as well as for the delivery of highly classified systems. # Verification and Validation Verification and validation are critical processes that ensure defense-related articles and services meet U.S. government requirements. These activities involve inspecting and testing these systems to confirm their performance and capabilities. ==========Naval research facilities across the US, located in places like Pensacola, FL and San Diego, CA, conduct vital medical and engineering research. These include: the Medical Research Center; Naval Dental Research Lab; Naval Health Research Center; and others. Other important locations are: Keyport, WA (Naval Undersea Warfare Center); Philadelphia, PA (Naval Surface Warfare Center); Newport, RI (Naval Undersea Warfare Center); Orlando, FL (Naval Air Warfare Center Training Systems Division); and Natick, MA (Naval and Clothing Textile Research Facility). Additionally, there are research facilities at the Naval Facilities Engineering Service Center in Port Hueneme, CA; and the Naval Submarine Medical Research Laboratory in Groton, CT. AEGIS sites can be found at Wallops Island, VA and Morristown, NJ.