

# *DoD Anti-Tamper Executive Agency*

---

## Anti-Tamper Overview and V&V Process



NDIA Systems Engineering Conference

Major James Yurack

October 2006



# Why AT? Combat Losses



**AT Protects US Critical Information  
and Technology From Being  
Exploited**



UNCLASSIFIED

# Why AT? Export Sales



**AT Serves as an Enabler to Improve Coalition Warfighting Capability**

UNCLASSIFIED



# Overview



- **AT Definition**
- **Implementation**
- **Policy**
- **Structure**
- **V&V Process**
- **Security**
- **Points of Contact**
- **Summary**



# *Anti-Tamper Definition*



- **System engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system.** DoDD 5200.39
  
- **AT protects information and technologies which lessens the likelihood of:**
  - **Countermeasure Development**
  - **Unwanted Technology Transfer**
  - **FMS/DCS systems being modified to increase their capabilities beyond export license limitations**

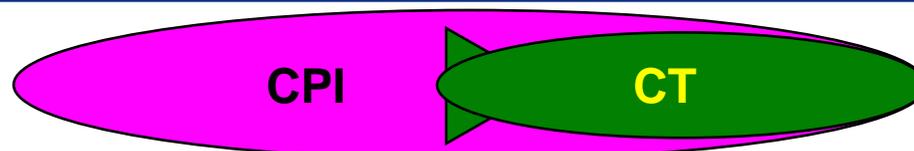
**Think about what you are trying to prevent or protect related to your program**

UNCLASSIFIED



# *Anti-Tamper Implementation*

## *What to Protect – Your Critical Technologies*



- **Critical Program Information (CPI) (DoDD 5200.39)**
  - ... technologies, applications... that, if compromised, would:
    - Degrade system combat effectiveness
    - Compromise the program or system capabilities
    - Shorten the expected combat-effective life of the system
    - Significantly alter program direction; or
    - Require additional RDT&E resources to counter impact of CPI compromise
  - Includes classified... information or controlled unclassified information restricted by statutes (e.g., export controlled data, intellectual property, trade secrets)
- **Critical Technology (CT)**
  - CPI located within a weapon system, maintenance system and/or training devices protected with Anti-Tamper technology

UNCLASSIFIED

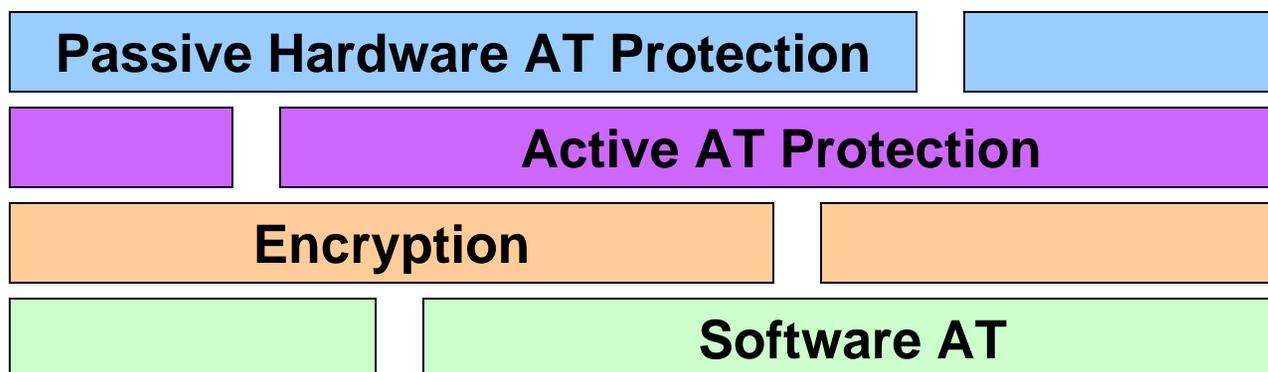


# *Anti-Tamper Implementation*

## *How to Protect – Use a Systems Engineering Mindset*



- **Make AT Part of the Systems Engineering Design & Development Process**
  - Less expensive during design
  - Difficult to retrofit effectively after development
- **AT Techniques are Varied & Evolving**
  - Counter to sophisticated threat
- **Multi-Layered Approach**





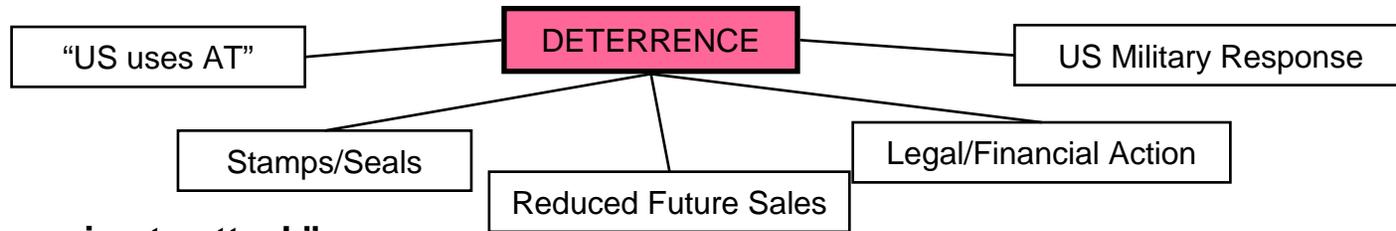
UNCLASSIFIED

# Anti-Tamper Implementation

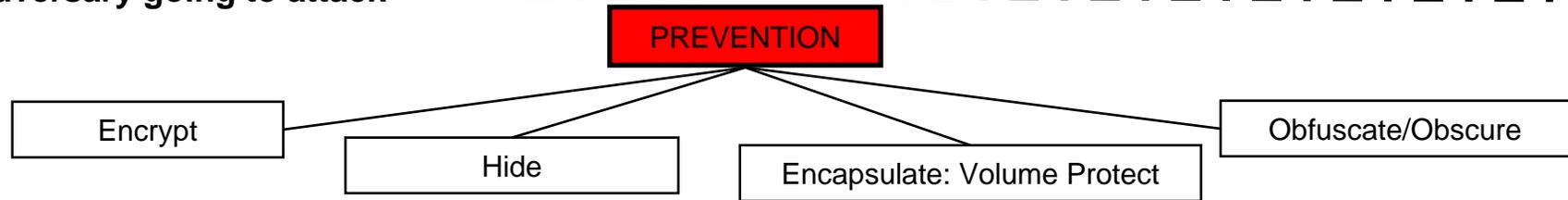
## Objectives - Deter, Prevent, Detect, Respond



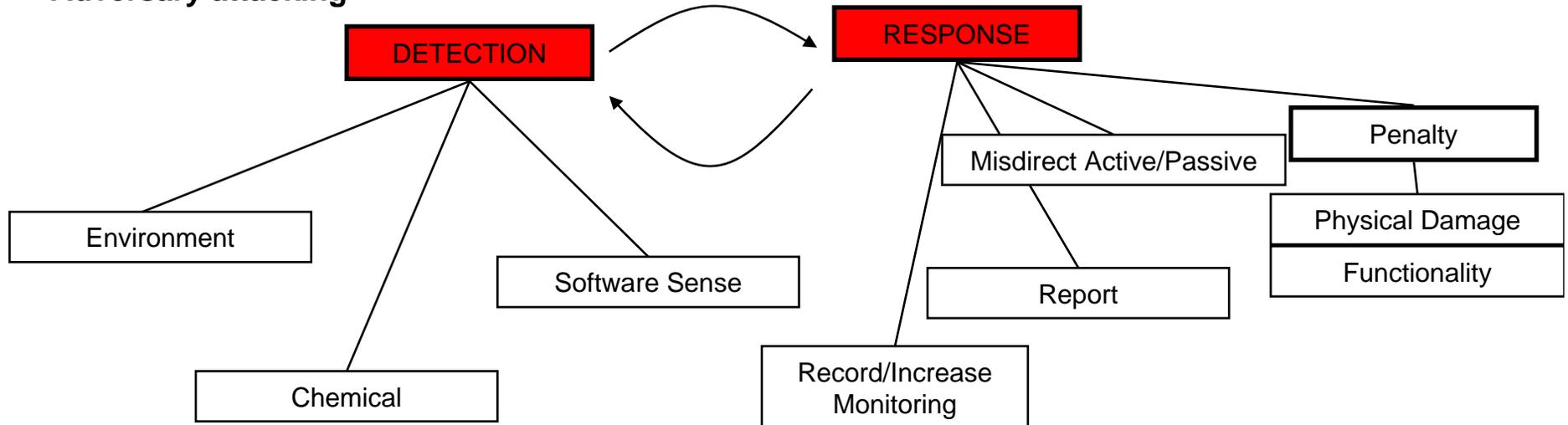
“Adversary thinking about an attack”



“Adversary going to attack”



“Adversary attacking”



UNCLASSIFIED



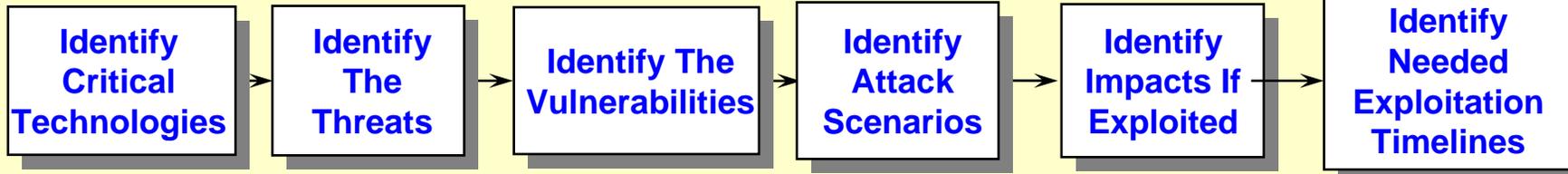
UNCLASSIFIED

# Anti-Tamper Implementation



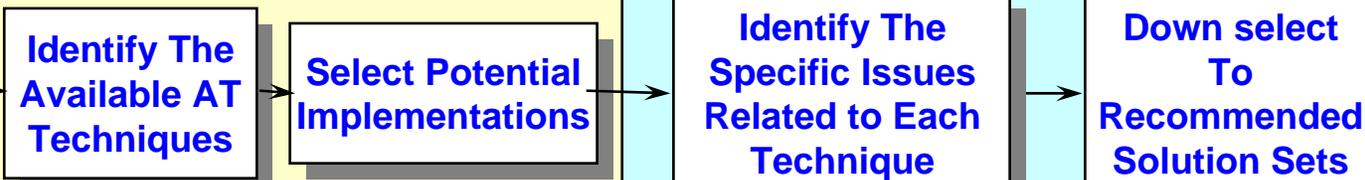
For Milestone B

**Develop an Exploitation Estimate Without Anti-Tamper**  
SPO/Cont/Exploiters Determine If Project Needs Protection & Amount



For CDR

**Determine Appropriate Solution to Meet the Need (s)**



UNCLASSIFIED

UNCLASSIFIED



# *Anti-Tamper Implementation*

## *What AT is Not*



- **No silver bullets**
- **Not a substitute for other security practices**
- **No global solutions that apply to all systems/scenarios**
- **Not an impenetrable defense**
- **Not just for FMS - Peacetime/crisis/combat loss may require AT for US system protection**

**AT is the last line of defense protecting your CT's after it is beyond the protection of guns, gates, and guards**

UNCLASSIFIED



UNCLASSIFIED

# Initial Anti-Tamper (AT) Memos

Issued by USD (AT&L)



Feb 1999 – “Implement AT in Acquisition Programs”

May 2000 – “Guidelines for Implementation of AT”

Jan 2001 – “AF as Executive Agent”

THE UNDER SECRETARY OF DEFENSE  
3010 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-3010

ACQUISITION AND TECHNOLOGY

04 FEB 1999

MEMORANDUM FOR SECRETARY OF THE ARMY  
ATTN: ACQUISITION EXECUTIVE  
SECRETARY OF THE NAVY  
ATTN: ACQUISITION EXECUTIVE  
SECRETARY OF THE AIR FORCE  
ATTN: ACQUISITION EXECUTIVE  
COMMANDER IN CHIEF, UNITED STATES SPECIAL  
OPERATIONS COMMAND  
ATTN: ACQUISITION EXECUTIVE  
DIRECTOR, BALLISTIC MISSILE DEFENSE ORGANIZATION  
DIRECTOR, STRATEGIC AND TACTICAL SYSTEMS

SUBJECT: Implementation of Anti-Tamper (AT) Techniques in Acquisition Programs

The Department of Defense policy encourages the sale or transfer of certain military equipment to allied and friendly foreign governments through the Foreign Military Sales Program and Direct Commercial Sales. The Department is also seeking increased foreign participation in programs from the requirements definition phase through production, fielding, and life-cycle management. While these efforts have the potential to enhance interoperability, standardization, and commonality, help reduce unit cost, and strengthen U.S. industry, they also risk making critical U.S. technologies potentially vulnerable to exploitation. Additionally, U.S. technology is exposed to loss over or in hostile territory.

The Department seeks to preserve the U.S. and Foreign Governments' investment in critical technologies through implementation of AT techniques and practices. Anti-Tamper is defined as "systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapons systems." The AT techniques are applicable to system performance, software, and hardware and are intended to delay rather than absolutely prevent exploitation. Anti-Tamper is based on existing DoD 5200.1M program security requirements and falls under the Special Access SENIOR CLUB Program recently approved by the Deputy Secretary of Defense.

I request that you accomplish the following steps to implement the AT techniques in acquisition programs and provide reports as follows:

a. Director, Strategic and Tactical Systems (S&TS):

(1) Assume OSD oversight, coordination, and policy responsibilities for AT within the Department of Defense.

THE UNDER SECRETARY OF DEFENSE  
3010 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-3010

ACQUISITION AND TECHNOLOGY

MAY - 1 1999

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Guidelines for Implementation of Anti-Tamper (AT) Techniques in Weapon Systems Acquisition Programs

The Department of Defense seeks to cooperatively develop weapon systems with its Allies and friends and to permit sales of weapon systems under the Foreign Military Sales program or via Direct Commercial Sales. Success in these areas will promote the Department's goals for standardization, commonality, and interoperability with foreign governments currently or likely to become coalition partners. Co-development, sales or transfer of weapon systems, and their potential loss on the battlefield will, however, expose critical U.S. technology to potential exploitation or reverse-engineering attempts. This unintentional technology transfer risk must be addressed by designing in AT measures to protect critical technology.

The attached "Guidelines for Implementation of Anti-Tamper Techniques in Weapon Systems Acquisition Programs" are effective immediately. The intent of this memorandum is to make routine in the acquisition process the deliberate assessment of the technologies involved in a weapon system development program, determine if the technologies are critical, and incorporate AT measures, if necessary, to protect critical technologies to the degree commensurate with operational and acquisition risk assessments. Anti-Tamper is required for all new start programs, all pre-planned product improvement (P3I) or other technology insertion efforts, and all programs that have not reached Milestone II as of this date. Anti-Tamper is not required for ongoing programs that are beyond Milestone II or in production, unless a P3I is involved or upon the determination of the responsible Milestone Decision Authority.

This is the foundation document for instituting AT in DoD's acquisition programs. It will be incorporated into the revision of the DoD 5000 series, the DoD 5200 series, the Defense Acquisition Deskbook, and the DoD Technology Protection Handbook.

J. S. Gantler

THE UNDER SECRETARY OF DEFENSE  
3010 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-3010

ACQUISITION AND TECHNOLOGY

05 JAN 2001

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Implementing Anti-Tamper (AT)

On May 1, 2000, I approved specific guidelines for implementing AT in the Department's weapons systems acquisition programs. Since that time, the Department has been moving forward with several actions to fully institute AT into the acquisition process. We have been exploring methodologies addressing AT policy and management, updating the DoD 5000-series documentation, determining effective testing strategies, and prioritizing efforts concerning AT technology development.

To ensure direct, effective coordination and implementation of AT activities between the Services, Government agencies/laboratories, and industry, and to avoid duplication of effort, I am designating the Air Force as the Department's Executive Agent for AT. Funds are being provided in the Fiscal Year 2002 budget to the Executive Agent to manage AT technology development, to implement policy, and to develop both an interactive AT databank/library and a technology roadmap that identifies, and prioritizes critical AT technology development needs. The Executive Agent will ensure accessibility to AT data, provide the proper security mechanisms, and conduct effective AT validation. AT validation is to be funded by specific programs.

The Services will continue to develop AT technology, maintain AT focal points, and implement AT technology into their respective weapons systems. The Services are responsible for funding the technology development and implementation necessary to protect individual weapon systems. The Director, Strategic and Tactical Systems, will continue to provide oversight and work directly with the Executive Agent and the Services, and will also coordinate with other OSD staff.

J. S. Gantler

DISTRIBUTION:  
SECRETARIES OF THE MILITARY DEPARTMENTS  
ATTN: ACQUISITION EXECUTIVES  
UNDERSECRETARY OF DEFENSE FOR POLICY  
COMMANDER IN CHIEF, UNITED STATES SPECIAL  
OPERATIONS COMMAND  
ATTN: ACQUISITION EXECUTIVE  
DEPARTMENT OF DEFENSE GENERAL COUNSEL

Initial memos established the requirements of AT, offered guidelines for implementing AT, and designated the Air Force as the AT Executive Agent

UNCLASSIFIED



UNCLASSIFIED

# Current AT Policy

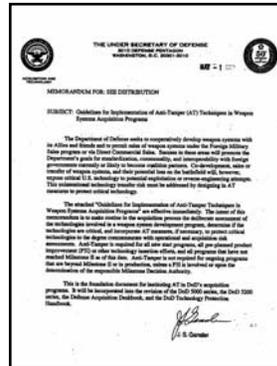
## Memos incorporated into existing documents



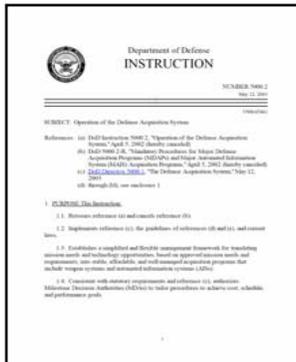
Feb 1999 – “Implement AT in Acquisition Programs”

May 2000 – “Guidelines for Implementation of AT”

Jan 2001 – “AF as Executive Agent”

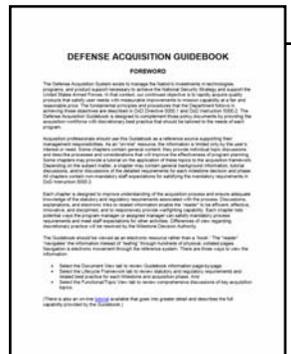


5000.2 – May 12, 2003



Sec 3.7 and 3.9

Defense Acquisition Guidebook



Chapter 8.5.3

5200.39 (Draft)– March 2002



Chapter 15

Updates to policy documents currently in work!

UNCLASSIFIED



UNCLASSIFIED

# *Proposed AT Policy*

## *High Lights*



- **All acquisition programs must identify Critical Program Information needing Anti-Tamper (AT) protection and document the results in the AT annex to the Program Protection Plan, including all**
  - **Programs presently exempt from the DoD 5000 series,**
  - **Advanced Concept Technology Demonstrations,**
  - **Foreign Military Sales and Direct Commercial Sales,**
  - **Pre-planned product improvement (P3I) or other technology insertion programs, and**
  - **Programs that have not reached Milestone C as of this date**
  
- **AT must be included in all acquisition program cost estimates.**

UNCLASSIFIED



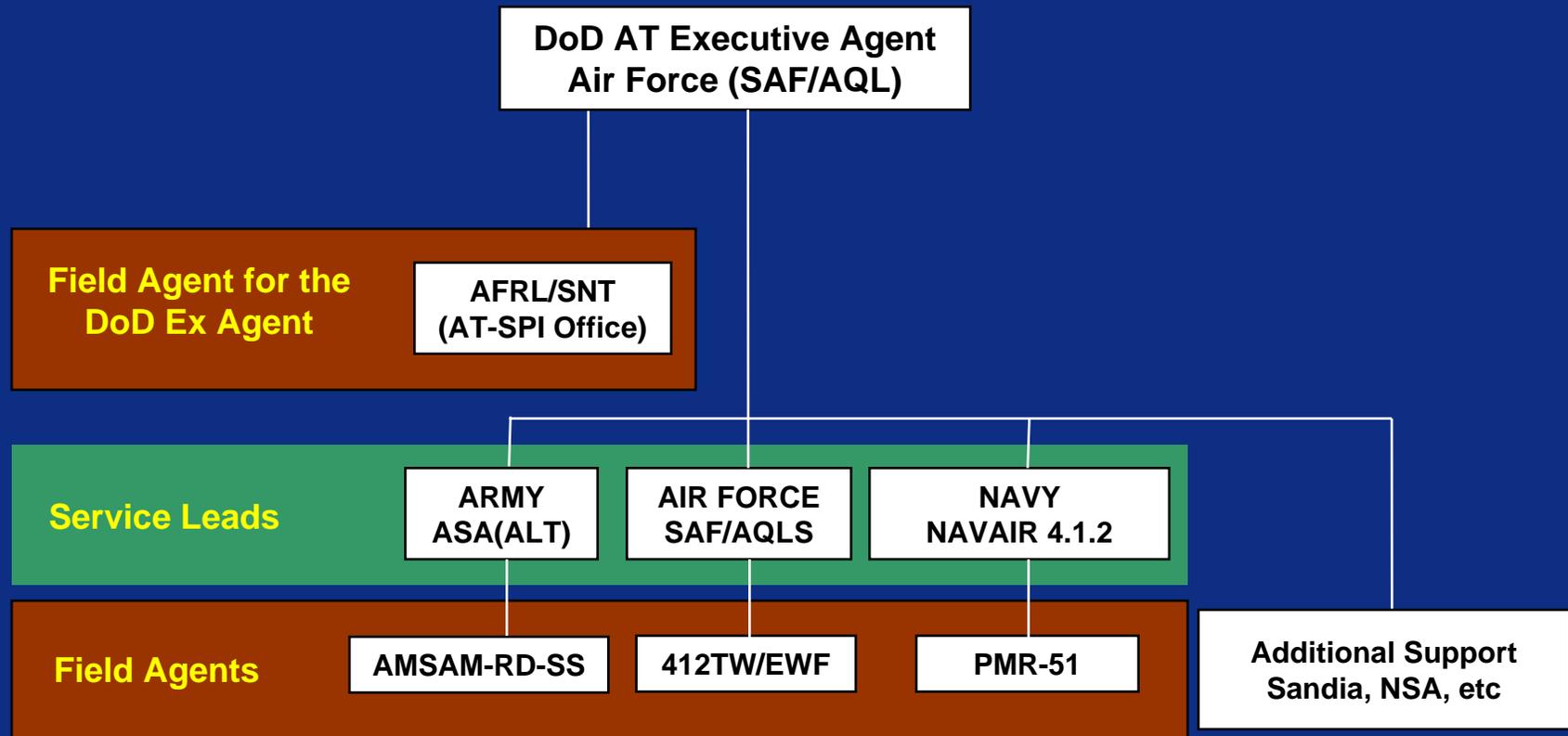
UNCLASSIFIED

# Anti-Tamper Support Structure

## Service Leads and Field Agents



### Anti-Tamper Structure



UNCLASSIFIED

UNCLASSIFIED



# *Anti-Tamper V&V Process*

## *V&V Team Roles*



- **V&V Team duties:**
  - **Validate the AT Plan**
    - Evaluate the AT design for providing sufficient protection
      - “Build the right thing”
    - Involvement helps ensure horizontal protection of CPI’s within DOD
  - **Verify the AT implementation**
    - Insures AT is installed and performs as expected
      - “Build the thing right”
  - **V&V team is NOT a Red Team**
    - Perform a consulting role
    - Not trying to “crack into” your system

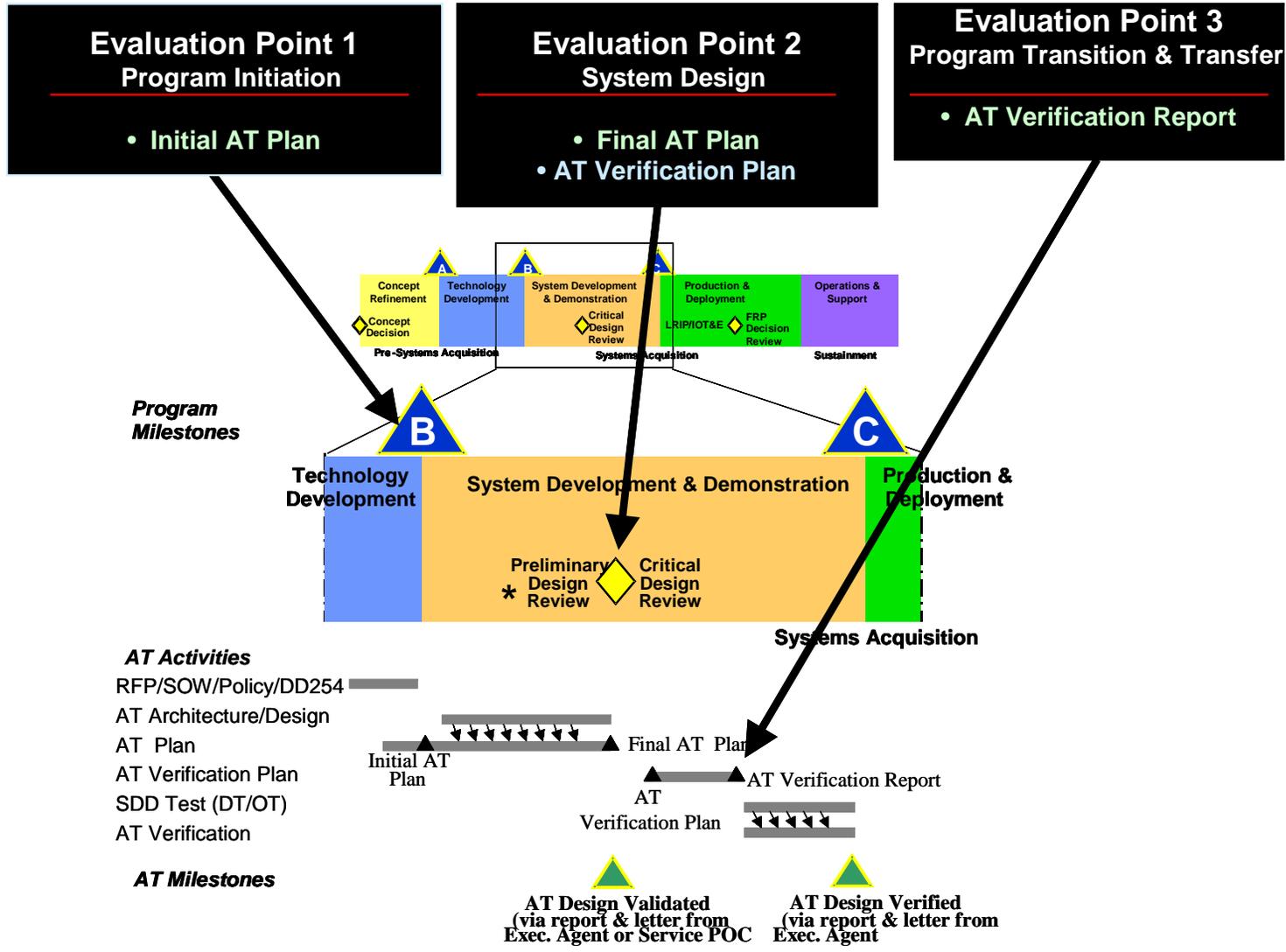
UNCLASSIFIED



UNCLASSIFIED

# Anti-Tamper V&V Process

## 5000 Series



UNCLASSIFIED

UNCLASSIFIED



# *AT Security*



- DoD ATEA has security architecture to support SAP and collateral protection
- Tools are being developed to assist programs make that determination

UNCLASSIFIED



UNCLASSIFIED

# ***AT Points of Contact***

## ***E-Mails and Websites***



- **DoD Executive Agent for AT**
  - **Email: [ATExecutiveAgent@pentagon.af.mil](mailto:ATExecutiveAgent@pentagon.af.mil)**
  - **Website: <http://www.at.dod.mil>**
  
- **Air Force**
  - **Email: [USAFATServiceLead@pentagon.af.mil](mailto:USAFATServiceLead@pentagon.af.mil)**
  
- **Army**
  - **Email: [Army.AT.Lead@rdec.redstone.army.mil](mailto:Army.AT.Lead@rdec.redstone.army.mil)**
  
- **Navy**
  - **Email: [NavyAT\\_Techagent@onr.navy.mil](mailto:NavyAT_Techagent@onr.navy.mil)**

UNCLASSIFIED



# ***SUMMARY***



- **Anti-Tamper protects critical technologies from being exploited**
- **AT must be part of systems engineering process**
  - **Up front and early**
- **AT is the responsibility of the Program Manager to implement**
- **Questions?...Call Service POC or DoD ATEA!**