

Welcome
to

TSA

Vaughn McCall 10/10/09

NOT THE
TRANSPORTATION
SECURITY
ADMINISTRATION

Vaughn McCall 10/10/09

but

Technology Security Associates

Vaughn McCall 10/10/09

PROGRAMMATIC **SECURITY SOLE 2009**

Vaughn McCall 10/10/09

INTRODUCTION

- Elements of Programmatic Security
 - Program Security
 - Anti-Tamper
 - Information Assurance

Vaughn McCall 10/10/09

- Elements of Programmatic Security
 - **Program Security**
 - Anti-Tamper
 - Information Assurance

Vaughn McCall 10/10/09

Program Security

- Program Protection
 - Critical Information Protection
- Program Protection Plan (Government)
Critical Program Information
- Program Protection Implementation Plan
(Contractor)

Vaughn McCall 10/10/09

Program Protection: Program Protection starts during the Concept Development / Refinement phase of a program. The programs plan is developed to identify / protect critical program information. By establishing early on that the developmental program could contain corporate propriety or critical military information adequate safeguards can be established.

To provide uncompromised and secure military systems to the warfighter by performing comprehensive protection of Critical Program Information (CPI) through the integrated and synchronized application of Counter Intelligence (CI), Intelligence, Security, systems engineering, and other defensive countermeasures to mitigate risk. Failure to apply consistent protection of CPI may result in the loss of confidentiality, integrity, or availability of CPI, resulting in the impairment of the warfighter's capability and DoD's technological superiority.

Program Security

- Program Protection Critical Information Protection
- Program Protection Plan (Government)
Critical Program Information DoDI 5200.39
- Program Protection Implementation Plan (Contractor)

Vaughn McCall 10/10/09

To mitigate the exploitation of CPI, extend the operational effectiveness of military systems through application of appropriate risk management strategies, employ the most effective protection measures, to include system assurance and anti-tamper (AT), and document the measures in a Program Protection Plan (PPP) (DoD 5200.1-M, "Acquisition Systems Protection Program,")

To conduct comparative analysis of defense systems' technologies and align CPI protection activities horizontally throughout the Department of Defense.

<http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf>

Program Security

- Program Protection Critical Information Protection
- Program Protection Plan (Government) Critical Program Information (cont)
- Program Protection Implementation Plan (Contractor)

Vaughn McCall 10/10/09

To identify CPI early in the technology development, acquisition, and sustainment process; refine at each milestone or as directed by the Milestone Decision Authority (MDA); and to initiate and maintain the appropriate protection of CPI throughout its military life cycle.

To require all research, development, and acquisition (RDA) programs with CPI to submit a PPP for review and approval by the appropriate MDA or science and technology (S&T) equivalent per (DoDI 5000.02, "Operation of the Defense Acquisition System,")

To assure federally funded products of fundamental research remain unrestricted to the maximum extent possible according to National Security Decision Directive 189 (National Security Decision Directive 189, "National Policy on the Transfer of Scientific, Technical, and Engineering Information,")

Critical Program Information

- Determining CPI
 - 20 Feb 08 Memo “Required Use of Standardized Process for Identification of the ID of CPI in DON Acq. Programs
 - DON CPI Tool
- Developing the Program Protection Plan for CPI

Program Security

- Program Protection Critical Information Protection
- Program Protection Plan (Government) Critical Program Information
- Program Protection Implementation Plan (Contractor)

Vaughn McCall 10/10/09

If a PPP has been identified as a requirement because of CPI, the Prime contractor will be required to develop a Program Protection Implementation Plan (PPIP). The PPIP should contain the following information as a minimum: A section detailing the Contractors overall approach to the PPIP and what general methodologies will be applied to the protection requirements described PPIP. The Contractor should also develop and implement the PPIP to ensure effective and efficient protection of Critical Program Information, technologies and systems, which shall include (at a minimum) the following: There is an existing PPIP DID which is of little value in developing a PPIP

- Elements of Programmatic Security
 - OPSEC
 - Program Security
 - **Anti-Tamper**
 - Information Assurance

Vaughn McCall 10/10/09

Anti-Tamper

- Anti-Tamper (AT) encompasses the systems engineering activities
 - delay exploitation / reengineering (RE) of HWCI / SWCI CPI in weapon systems.
 - involve the entire life-cycle of systems acquisition, including research, design, development, implementation, manfg, testing of AT measures and reclamation.

Vaughn McCall 10/10/09

Anti-Tamper (AT) encompasses the systems engineering activities intended to prevent and / or delay exploitation / reengineering (RE) of Hardware / Software Configuration Item (HWCI / SWCI) identified as containing Critical Program Information (CPI) in U.S. weapon systems. These activities involve the entire life-cycle of systems acquisition, including research, design, development, implementation, manufacturing, testing of AT measures and reclamation.

Anti-Tamper

- CPI is information (DoDI 5200.39) concerning research, science, technologies, program information, processes, applications, algorithms, hardware, software, or system end items that, if compromised, would;
 - (1) Cause significant degradation in combat effectiveness;
 - (2) Shorten the expected combat-effective life of the system;
 - (3) Reduce technological advantage
 - (4) Significantly alter program direction; or
 - (5) Enable an adversary to defeat, counter, copy or reverse engineer the technology or capability

Vaughn McCall 10/10/09

Anti-Tamper

- The Contractors Anti-Tamper Plan shall follow the current DoD ATEA AT Plan Template format (www.at.dod.mil). AT is developed incrementally with the initial plan due at the Program Design Review (PDR) and the final Plan at Critical Design Review(CDR). Unless effective presentation would be degraded, the initially used format arrangement shall be used for all subsequent submissions. The program AT critical technologies analysis described therein shall include those aspects of the foreign intelligence threat that are applicable to the specific contract. .

Vaughn McCall 10/10/09

Contractors Anti-Tamper Plan

- The Contractor shall use the DoD ATEA AT Plan Template.
- Additionally, as a minimum, the AT Plan portion shall contain
- Proposal AT Plan (Initial) shall be prepared and delivered as part of the Contractor's Contract Proposal. (System level (system performance requirements.)

Vaughn McCall 10/10/09

- Elements of Programmatic Security
 - OPSEC
 - Program Security
 - Anti-Tamper
 - Information Assurance

Vaughn McCall 10/10/09

Information Assurance

- Public Key Infrastructure (PKI)
- Classified Information
- Public Release
- Foreign Disclosure

Contractor shall obtain and utilize PKI certificates issued by approved External Certificate Authority (ECA), for the purposes of protecting all controlled unclassified information (CUI). A substitute to utilizing approved PKI ECA certificates is for the contractor to become a member of the Federal Bridge Certification Authority in order to issue approved contractor issued PKI certificates with trust relationships to the DoD PKI. Approved PKI will be utilized by the Contractor and their subcontractors when transmitting CUI via electronic means.

Information Assurance

- Public Key Infrastructure (PKI)
- **Classified Information**
- Public Release
- Foreign Disclosure

. All classified information transmitted by the Contractor shall be in compliance with DoD 5220.22-M, "National Industrial Security Program Operating Manual".

The Contactor shall address these requirements within the Program Protection Implementation Plan.

Information Assurance

- Public Key Infrastructure (PKI)
- Classified Information
- Public Release
- Foreign Disclosure

Government / Contractors shall ensure program related information and graphics intended for public release or posting on Internet and World Wide Web sites are processed through the PM Public Affairs Officer before release. The Government / Contractor shall include note pages in all briefings and slide presentations submitted to the PM Public Affairs Officer / Security Manager for review and release (re: SECNAVINST 5510.36A and DoDD 5230.9)

Information Assurance

- Public Key Infrastructure (PKI)
- Classified Information
- Public Release
- Foreign Disclosure

If the Program has foreign applicability, all information both Government / Contractor will be coordinated through the Navy International Program Office as well as the Programs Foreign Disclosure Officer before release to the applicable FMS Country