2010 NDIA T&E SYMPOSIUM OTA COMMANDERS' ROUNDTABLE

A Navy perspective on Information Assurance -having systems that work when needed

2 March 2010

Bill McCarthy Deputy Director Operational Test & Evaluation Force



Common Challenges

- "Cyber" is still a relatively new warfare domain
- The cadre of truly experienced personnel is small and while growing, will take literally years to fully develop
 - We are all competing for the same talent pool
- The threat is ubiquitous and is rapidly evolving
- There are often expectation mis-matches there is not necessarily agreement as to the goal or desired outcome of testing

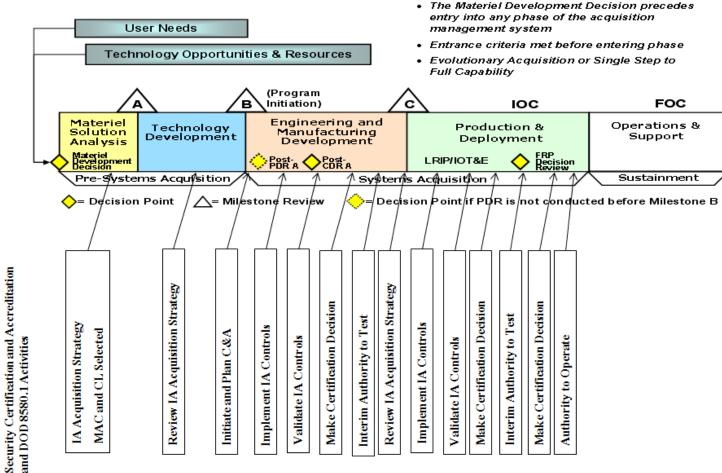


hallenges in Acquisition Life Cycle

- Upfront definition of IA requirements is a prerequisite for integrated testing
- IA controls "inheritance" is not understood by the implementing Program Manager
- Program Managers often fail to consider
 - IA in RFP, PDR, CDR, Contracts, CDRLs
 - Supply Chain Risks
- Integration Challenges
 - Need for realistic operational environment s with end-to-end test venues
- Current certification & accreditation process was not designed to support rapid software development
 - Process can be slow and inflexible
 - Process does not readily account for incremental changes
- System developers, certification & accreditation authorities, and testers need to collaborate and share IT test results
 - Program managers perceive they are paying several times for IA

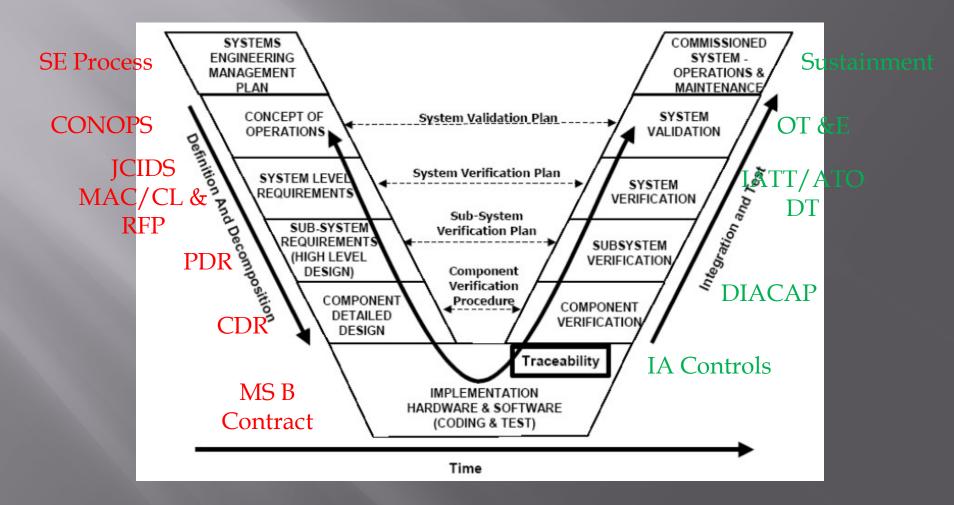


IA in the Acquisition Life





IA in the "Notional" Systems Engineering Life Cycle





Navy Challenges

- Ships are inherently high demand low density assets
- Most legacy platforms (ships, in particular) are an amalgamation of systems
 - Legacy hardware & software
 - COTS and open source code
- Individual platforms are limited in number and often rely upon a relatively small set of interface points to connect with the GIG.



Some thoughts...

- IA/CND test and evaluation requires a holistic approach that views contractor testing, government DT and OT as a continuum
 - Program Managers must work to integrate Government and Contractor Developmental Testing
- The evaluation strategy must be based upon sound architectural views that provide sufficient rigor
 - The OT&E community should support JFCOM efforts to improve the quality of net-centric architectural views
- New tools must be developed to support the collection of system performance data without unduly impacting the performance of the system under test
- A new paradigm for examining how we assess the ability of our systems to support combat operations in the face of cyber attack is needed

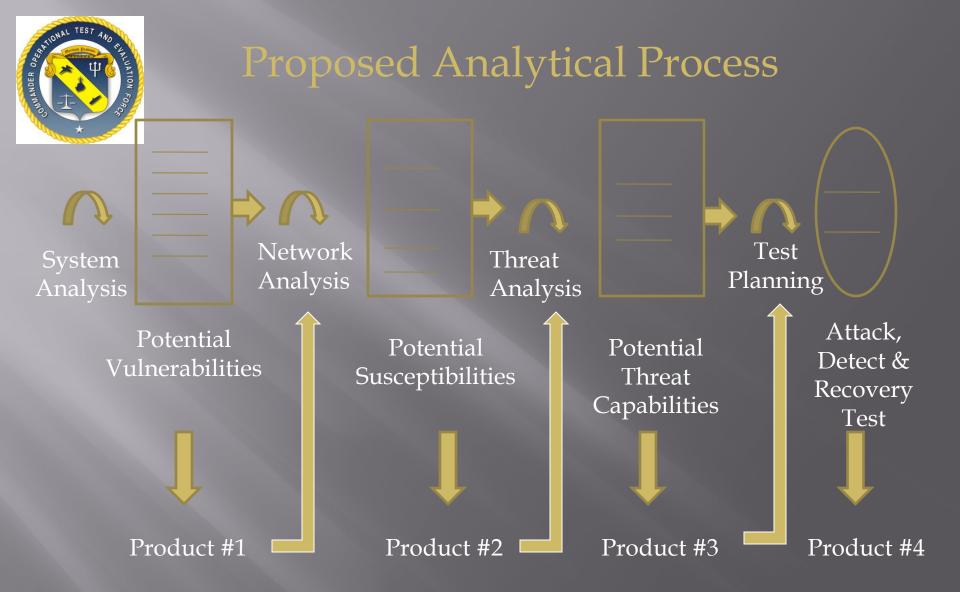


A Suggested Analytical Process

- **Determine the** *criticality* of the system and the security *required*
- Assess non-physical and physical vulnerabilities
- Consider <u>susceptibility</u> to *espionage*, *disruption* or *malicious manipulation*

■ Assess threat <u>capability</u> and test using the types of exploits likely to be encountered in the operational environment

■ Assess <u>recovery</u> and repair, (recognizing that unlike kinetic attack, *detection of the attack may not be obvious*.)





Summary

Challenges are similar, yet different:
Well defined requirements
CONOPS
Instrumentation

Skilled personnel

Bottom line – we are confronted with a rapidly evolving warfare domain with associated risks and opportunities - we need to get this right!

IA Policy and Guidance...Voluminous!

ATIONAL TEST AND

MMANDER C

ENALUATION

Build and Operate a Trusted GIG Cyber, Identity & Information Assurance (CIIA) Related Policies and Issuances CYBER, IDENTITY & INFORMATION ASSURANCE Developed by DASD-CIIA Last Updated: November 10, 2009 DOD Cyber, Identity & Inform Assurance Stratenic Plan DoDD 8500.01E Information Assurance (IA) DoDI 8500.2 Information Assurance Implementation Management of the DOD information AUTHORITIES Send questions/suggestions to iatac@dtic.mil DD 8100.0 ASD(NE)/DoD CIO G&PM 11-8450 DVD GIG Committee Title 14 Cooperation With Other Agencies (Ch. 7.85 141, 144, 145, 148, 149, 150 Global Information Grid (GIG) DoD CIA Campaign Plan Armed Forces (953013(b), 5013(b), 8013(b) Title 32 National Guard (§102) Title 40 Public Buildings, Property, and Work (Ch. 113: §§11302, 11315, 11331) CIIA GOAL 1: ORGANIZE CIIA GOAL 3: ANTICIPATE CIIA GOAL 4: PREPAR CIIA GOAL 2: ENABLE 1.1 Lead and Govern in Uncertainty 2.1 Secure Data in Transit 3.1 Understand the Battlespace 4.1 Develop and Maintain Trust. Title 50 War and National Defense (\$5401, 1801) Title 44 Public Printing and Docum (Ch. 35: §§3541, 3504) ation Files Manag Similario Phan (Deal) ASDIMENDOD CKO DoD PISNA Guidance - Filsoni Year 2009 DoDD 8521.01E DoDI 8523.01 communications Security (COMSEC DoDD 8115.01 IT Portfolio Management landerds for Security Categori of Federal Info. and Info. Syst deline for identifying an inform Federal Information Security regement Act, 44 U.S.C. \$3541 et OUSD() Marrio OUSD() Marrio Availables (BA) -Clinger-Cohen Act, Pub. L. 104-105 DoDI 3-5200.16 loctives and Min Sids for COMSEC Measures used in NC2 Comms SP 800-18 Juide for Developing Security Plan DoCI 4850.1 Policy and Procedures for Mgt and Us of the Electroneurostic Scientism SP 800-80 Guide for Mapping Types of Info and Info Systems to Security Categories 4.2 Strengthen Cyber Readiness IT Portfolio Managament Bath Canability Area Case UCP Unified Command Plan (US Constitution Art II, Title 10 & 50) DoDD 4640.13 SP 800-30 Guide for Conducting Risk CJCSI 6510.02C DoDD 7045.20 Cepability Portfolio Management COMSEC Monitoring and Information Assumation Readiness Testing A Policy for Space Systems Used by The DoD Mgt of Base and Long Haut accounts Equipment and Sarvi Cryptographic Modernization Plan 3.3 Prevent 3.2 Prevent and CJC31 8510.06A NSTISSD-800 NATIONAL / FEDERAL DeDI 7000.14 CJC8 3170.01G CNSSI-5000 Guidelines for Voice Over Internet fotocol (VoIP) Computer Telephon Delay Attackers... Attackers from Staying DoDD 3100.10 800 inty (COMSEC Communications Se Financial Management Policy and Proceedules (PPSE) Joint Capabilities Integration and Development System (JCIDS) nications Security Releases Space Policy Monitoring NSD-42, National Policy for the Security of Nati Security Telecom a Information Systems Foreign Mellons CN851-4009 CARPED 12 National Information Assumnos Glossery NACSI-6002 Neff COMSEC Instruction Protection Gov1 Contractor Telecomm's DoDD O-8530.1 Computer Network Defense (CND) DoDD O-5100.30 Department of Defense (DoD) Command and Control (C2) Vational IA Policy for Space System Used to Support NSS Type-Acceptance Program for VolP 1.2 Design for the Fight CNSSD-502 National Directive On Security of National Security Systems NSPD 54 /HSPD 23 Computer Security and Monite NCSC-5, Nat'l Policy on Use of Pyptometerial by Activities Operating In High Risk Environments DoDI O-8530.2 Support to Computer Network Defense (CND) DoDD S020.40 Defense Chilical Infrastructure Protection Program National Policy on Securing Voice DoDD 5000.01 The Defense Accusition System NSSD-800, Governing Procedures the Committee on National Security Systems Information Assurance (IA) in the Defense Acquisition System A-130, Management of Fed Info Resources, Appendix III, Security of Fed Automated Info Ses DoD C-8530.1-M CND Service Provider Certification and Accreditation Program DoDI 8510.01 DOD IA Certification and Accreditatio Process (DIACAP) DoDI 5000.02 Son of the Defense Acquisitor NSTISSI-7003 Tolective Distribution Systems (PD6 National Policy for Safeguarding and Control of COMISEC Material 4.3 Sustain Missions CNS8D-90 art Security Telecomm's and Info Sy Security (CNSS) Issuance System National Security Stralegy DoDi 8551.1 Ports, Protocsis, and Services Management (PPSM) CNSSP-17 National Information Assurance Policy on Wireless Capabilities FIPS 140-2 Security Requirements for Crystocrastic Modules ponent of the GIG Integn Architecture, v1.1 National Information Assurance Acquisition Policy DoDD C-8200.19 National Instruction on Classified NSTISSI-4002 Classification Guide for COMSEC ontrol of Compromising Empir FAR Federal Acquisition Regulation DoDI 8552.01 Use of Mobile Code Technologies in DOD Information Systems CNSSI-4004, Destruction and sergency Protection Procedures I COMSEC and Class. Material CNSSP-18 National Policy on Classified Information Spillage ASD(MI)/DoD CID G&PM 12-8430 Acquiring Commercial Software National Policy Governing the Use of HAIPE Products National Policy on the Use of AES to Protect National Security Systems. _ National Strategy to Secure Cyberspace CJCBI 6510.01E Information Assurance (IA) and Computer Network Defense (CND) National Datense Strategy (NDS) CNSSP-25 National Policy for PKI in National Security Systems ASD(NII)/DoD CIO Memo Use of Commercial Wireless LAN evices, Systems, and Technologies ASD(NE)/DoD CIO Memo DOD Support for the SmartBUY CN58P-22 CNSSP-8 National Policy for CSA of National Security Telecom and Info Systems IA Risk Management Policy for National Security Systems National Military Strategic Plan for the War on Terrorism CJCSM 6510.01A Information Assurance (IA) and Computer Network Defense (CND) National Military Strategy (NMS) MAC 84,2005 VACSI-2005, Foreign Millery Sales o COMSEC Articles and Services to Foreign Gov'ts and Inti Orga DFARS tpert 208.74, Enterprise Soft CJCSI 6212.01E eroperability and Supportability of I and National Security Systems IN ROOMSER CNSSP-21 National IA Policy on Enterprise Architectures for NSS DoDD 3020.44 Defense Crisis Manapement Fort Dam Medic National Milliony Strategy for Cyberspace Operations (NMS-CO) Quadrennial Defense Review (QDR) ASD(C3) Policy Men DoDD 8100.2 Use of Commercial Write Services, and Tech in Tech NS71557-400 Federal Desistop Core Configuration Guidance for CND Response Action Common Criteria Evaluation and Validation Scheme (CCEVS) Controlling Authorities for COMSEC DoDD 3020.28 Department of Defense Continuity Programs CNS SP-300 National Policy on Control of Compromising Emenations Framework for the GIG (ture (AFG) version 1.1 (PDCC) ASD(M)/DxD CIO Mento National Military Strategy to Combat Guidance for Development of the Force (GDF) for 2010-2015 DoDD 4830.05 Inimum Security Requirements for Federal Information Systems Protection of Sensitive DoD Date a Weapons of Mass Destruction 2.2 Manage Access Rest on Portable Computing Device SDINIDDoD CIO Memo, Encryptic DoDD 5144.1 ASD for Networks and Information Integration/DoD CIO **DIACAP Knowledge Service** NSTISSI-7001 NONSTOP Countermeasures operability and Supportability of I National Security Systems (NSS) Executive Order 13231 DTM 06-060 Palicy on Use of DoD into Sys -- Std Consent Barner and User Agreement. Executive Order 12958 willed Netional Security Inform Difficel Infrestructure Protec Information Age DoD 1000.25 DOD Personnel Identity Protection (PIP) Program of Unclass DAR on Mobile Comp Devices and Removable Storage Public Key Infrestructure (PKI) and Public Key (PK) Enabling 240.02.3000 Defense Acquisition Guidebook Section 7.5 Information Assurance Presidential Memo, "Classified TEMPEST Countermeasure for 1.3 Develop the Workforce ASDINE VOID CRO Memo Computer Finaud and Abuse Act. Title 18 (§1030) Fackbas) information, 27 May 09 HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors DoD Strategic Plan for identity DoDI 8410.02 DOD 8570.01-M Information Assurance Workforce Improvement Program NSTISSI-7002 TEMPEST Closency NetCos for the C IA Training, Certification, and Federal Wiretep Act Title 18 (§2510 et seq.) Foreign Intelligence Surveillance Act. Title 50 (\$1801 et sec) ASD/NI/DoD CIO Memo Approvil of Externel Public Key Internet or Approved M-05-24 Insplementation of HSPD-12 NSTISSI-4011 National Training Standard for INFOSEC Professionals Pen Registers and Trep and Trace National Training Program for INFOSEC Professioners Stored Communications Act. Title 18 (§2701 et seq.) Title 18 (§3121 et seq.) FIPS 201-1 versional identity Verification (PTV) recent Employees and Contractor Operational Security Doctrine for 8 FORTEZZA User PCMCIA Card CNSSI-4012 National IA Training Standard for Sanker Systems Managers Training Assurance (IA) Education NS3P-10, Nat'l Pokcy Governing Use Approved Security Containers In Info Sys Security Apps CNSSP-18 Halional Policy for the Destruction of COMSEC Paper Material OPERATION National IA Training Standard For formation Systems Security Officer National IA Training Standard Fo System Administrators (SA) Color Key - OPRs STRATCOM COMPLAN 8039-08 STRATCOM OPLANS HSTISSI-4010 Keying Melokel Menage ASTYNEYASTYCCU aleguarding COMSEC Facilities and ABOUT THIS CHART CNSSI-4016 ational IA Training Standard For Ris 1000 CIO \$1 507-0 ional Training Standard for Syster Certifiers CNRRNTIR NSTISSI-4003 Reporting and Evaluating COMSEC This chart organizes information assurance policies and guidance by CIIA Strategic Goal MSTISSI-4001 Controlled Cryptographic Nerra NSTISSI-4000 DISA and Office of Primary Responsibility (see Color Key). It is intended to show all IA or IA-Si 701-01 NelOps Reporti SD 527-01 ND INFOCON System OMSEC Equipment Maintenance related policies a Component may need to comply with and direct users to the full text. DNE CNSSP-3 istional Policy for Granting Access to Dessilied Cryptographic Information Crypto Modernizat for Type 1 Class JCS 1.4 Partner for Strength No priority is intended by the arrangement of the guidance boxes. NAP 2.3 Assure Information Sharing Policies in hatched boxes represent new or updated drafts with a release scheduled in the NSTISSI-1000 onel Information Assurance C&A Process (NBACAP) NIST ational Policy Governing the Release near future. Π NSA SUBORDINATE POLICY DeDD 8520.02 Data-Starting in a Net-Centric Department of Defense CJCSM 3213.02 Joint Staff Fooal Point CNSSI-4007 mmunications Security (COMSEC Utility Program 050 in the electronic version, each policy is hyperlinked to its full text online. To use the Togram for the Mgt and Use of Nat Reserve IA Security Equipment hyperlink, simply click on the box. rity Technical Implemer Quides (STICs) STRATCOM SP 800-39 Use of Peer-to-Peer File Sharing Applications Across DoD loss Domein Community Roads USD(AT&L) Oulde for Security Authorization of Federal Info Systems Policies in Italics indicate the document is marked for limited distribution or no public-facing Security Readiness Review Scripts Security Checklish USD(C) hyperlink is currently available. SP 800-53A inded Security Controls for al Information Systems ed States Intelligence Commun Information Sharing Strategy SP 800-53 R3 Inded Security Controls for **DoD Information Sharing Strategy** USDIN For printing, this chart is best viewed on 22"x17" (Size C) paper. Security Configuration Guidelines (SCCs) CJC8I 6211.02 DISA FSO Whitepapers DTM-06-087 USD(P) Security of Undessified DoD smallon on Non-DoD Into Syste CMSSI-1253 Security Controls Catalog (SCC) (Craft) Defense Information System Policy and Responsibility For the latest version of this chart go to http://lac.dtic.mi/latac/la_oolicychart.html. USD(P&R) Other Agencies DoD Strategic Plan for Defense tohothai Base Cyber Security and Information Association DoDr 5205.8 Defense incourse Base Cyber Security /14 Activities (Drate Distribution Statement A: Approved for Public Release. Distribution is unlimited.

Bill McCarthy Deputy, Operational Test & Evaluation Force Norfolk, VA 757.282.5546 Ext. 3900 William.mccarthy@cotf.navy.mil