Command & Control Center

Information Assurance Policy Cross Walk Out Brief

Prepared for

13 Annual NDIA Systems Engineering Conference

Net Centric Interoperability/Systems of Systems Track Session 4A3

Peter Christensen, Susan May, Vijay Rachamadugu, Robert Smith

With Guidance from:

Mr. Ralph Harris OSD DOT&E, Ms. Darlene Mosser-Kerner AT&L DT&E

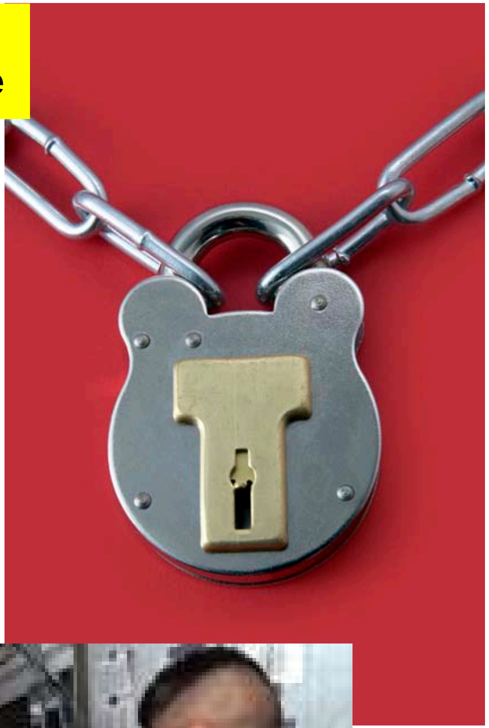
28 October 2010

MITRE

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Information Assurance (IA)
Policy Cross Walk: Bottom Line

IA must be addressed early and throughout the acquisition lifecycle to ensure successful IA OT&E and a Secure and Resilient DOD Enterprise

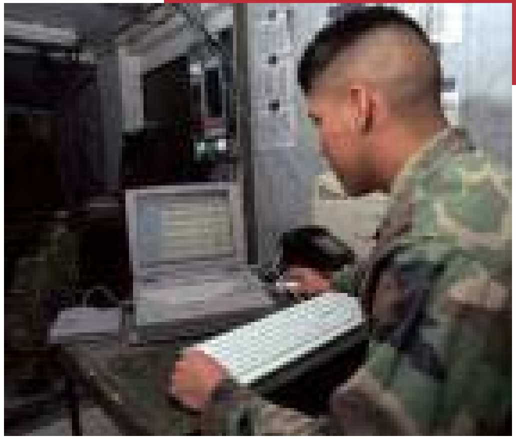


- **Address IA Capabilities Earlier and Throughout System Development Lifecycle**

- **Develop Overarching, Unified Framework for IA Requirements, Contracting, Engineering, and Testing**

- **Form Integrated Test Teams Early**
  - Promote Collaboration among Acquisition, Engineering and Test Teams
  - Enables "test by one, use by many"

- **Promote Acquisition-Related IA and Computer Network Defense (CND) T&E as Critical to Ensure Secure DOD Systems**
  - Provide Adequate Resources & Expertise Essential for Testing
  - Operationally Realistic IA Test Environment is Crucial to Successful Testing
  - Threat Portrayal During Testing Must Reflect Current Threat Information



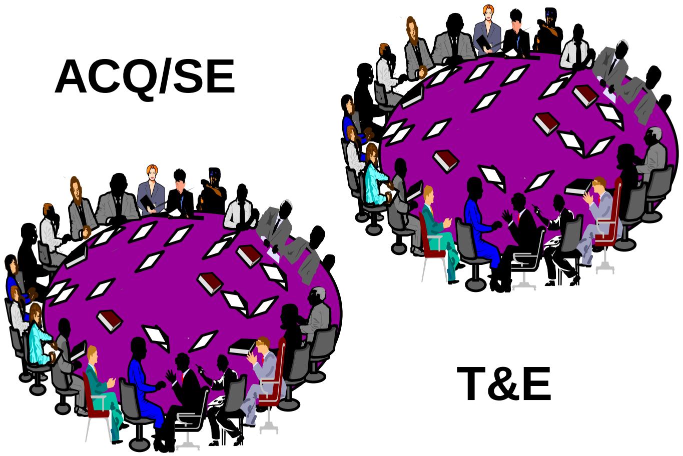
Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Working Group Background

- **OSD Test & Evaluation WG Identified Need to Address IA Deficiencies**
- **IA Policy Crosswalk Working Group Charter signed 20 May 2009**
  - Mr. Chris DiPetto, OUSD DDT&E
  - Mr. W.J. McCarthy, OSD DOT&E
- **Charter Phases and Results**
  - **Phase I**: Examine current IA related T&E policies, directives, instructions and guidance
    - Identify duplication, conflicts and gaps
    - Take a broader look beyond just T&E
      - Explore “Test by one, accept by all”
  - **Results**: Team summarized findings for T&E Executives Fall 2009
  - **Phase II**: Produce recommendations
    - Focus on coordinating IA Test and Evaluation Activities
      - Streamlining, reuse, and tailoring of test requirements
  - **Results**: Report submitted to T&E Executives for review and appropriate action

Phase II Sub Groups and Participants

- **Two Sub Groups Formed**
  1. IA in Acquisition and Systems Engineering
  2. Collaborative IA T&E
- **Groups categorized issues in each area**
  - Evaluated alternatives
  - Developed specific recommendations

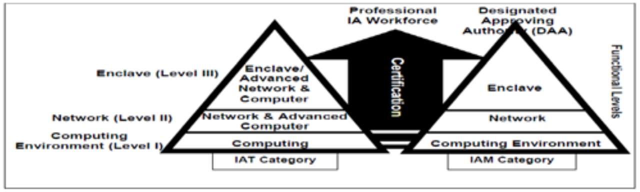


Name	Organization	Name	Organization	Name	Organization
Abeyta, Derek	Air Force	King, Art	OSD-NII/CIO	Subramonian, Nat	Contractor-IDA
Adams, Nate	MITRE	Krammes, Shannon	USMC	Tobias, Mariann CIV	AFMC ESC/AQT
Artis, Mike CIV	DISA, TEMC	Kulas, Ed	Air Force	Tucker, Timothy	Navy
Avey, Thomas	MITRE	Landin, Dan	Army	Tuteral, David	OSD-NII/CIO
Beck, Robert	Contractor-Wyle	Leiby, Larry CIV	Army DUSA TEO	Wells, Shelly	J6
Beech, Ed	Navy	MacBrien, Andy	USAF ESC Engineering	York, Jack	Air Force
Berger, Robert	OSD-AT&L	Manthei, Jerry	Contractor, Navy		
Burgess, Larry	USMC	Matthews, Steve	MITRE		
Christensen, Pete	MITRE	Mattison, Dennis CIV	Navy-SPAWAR		
Clark, Michael CIV	Army ATEC	May, Susan	MITRE		
Combs, Jeffrey	USMC	Miller, John	MITRE		
Cox, David	USMC	Morris, James	Air Force		
Dahmann, Judith	MITRE	Mosser-Kerner, Darlene	OSD-AT&L		
Davis, Michael H CIV	Navy-SPAWAR	O'Connor, Martha	OSD-AT&L		
Davis, Michael FCIV	USMC	O'Connor, Patrick	Army		
Garrett, Douglas	OSD/ATL	Phillips, Michael	Air Force		
Harris, Ralph	OSD-DOT&E	Rachamadugu, Vijay	MITRE		
Holmes, Kevin CIV	DISA, JITC	Shanahan, Ray	OSD		
Johnson, Melody	Air Force	Smith, Bob	MITRE		
Kiesel, Kenneth CIV	DISA, JITC	Spinella, Edmund CIV	USMC		

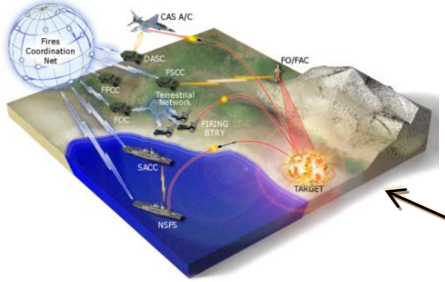
Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Issues Addressed
IA Policy Cross Walk Report

IA Policy, Guidance and Work Force Training


Professional IA Workforce
Designated Approving Authority (DAA)
Enclave (Level III)
Enclave/ Advanced Network & Computer
Certification
Enclave
Functional Levels
Network (Level II)
Network & Advanced Computer
Network
Computing Environment (Level I)
Computing
Computing Environment
IAT Category
IAM Category

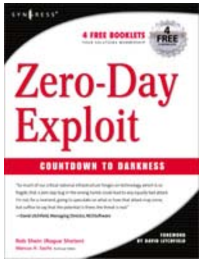
Contracting



Requirements Definition, Systems Engineering and Process Execution

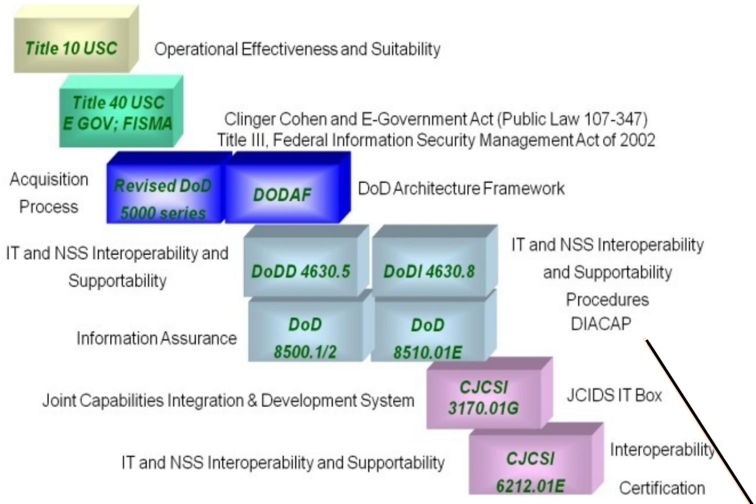
Platform IT

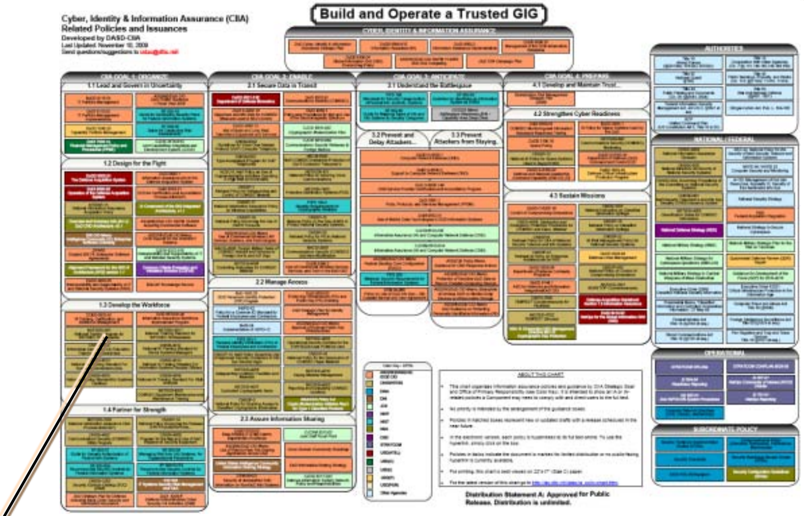
These issues collectively impede IA and Computer Network Defense T&E



Realistic IA and CND Test Environments and Resources

Issue: IA Policy and Guidance


Title 10 USC
Operational Effectiveness and Suitability
Title 40 USC
E GOV; FISMA
Clinger Cohen and E-Government Act (Public Law 107-347)
Title III, Federal Information Security Management Act of 2002
Acquisition Process
Revised DoD 5000 series
DODAF
DoD Architecture Framework
IT and NSS Interoperability and Supportability
DoDD 4630.5
DoDI 4630.8
IT and NSS Interoperability and Supportability Procedures
Information Assurance
DoD 8500.1/2
DoD 8510.01E
DIACAP
Joint Capabilities Integration & Development System
CJCSI 3170.01G
JCIDS IT Box
IT and NSS Interoperability and Supportability
CJCSI 6212.01E
Interoperability
Certification


Cyber, Identity & Information Assurance (CIA) Related Policies and Issuances
Developed by DASD-CIA
Last Updated: November 10, 2009
Build and Operate a Trusted GIG
Distribution Statement A: Approved for Public Release. Distribution is unlimited.

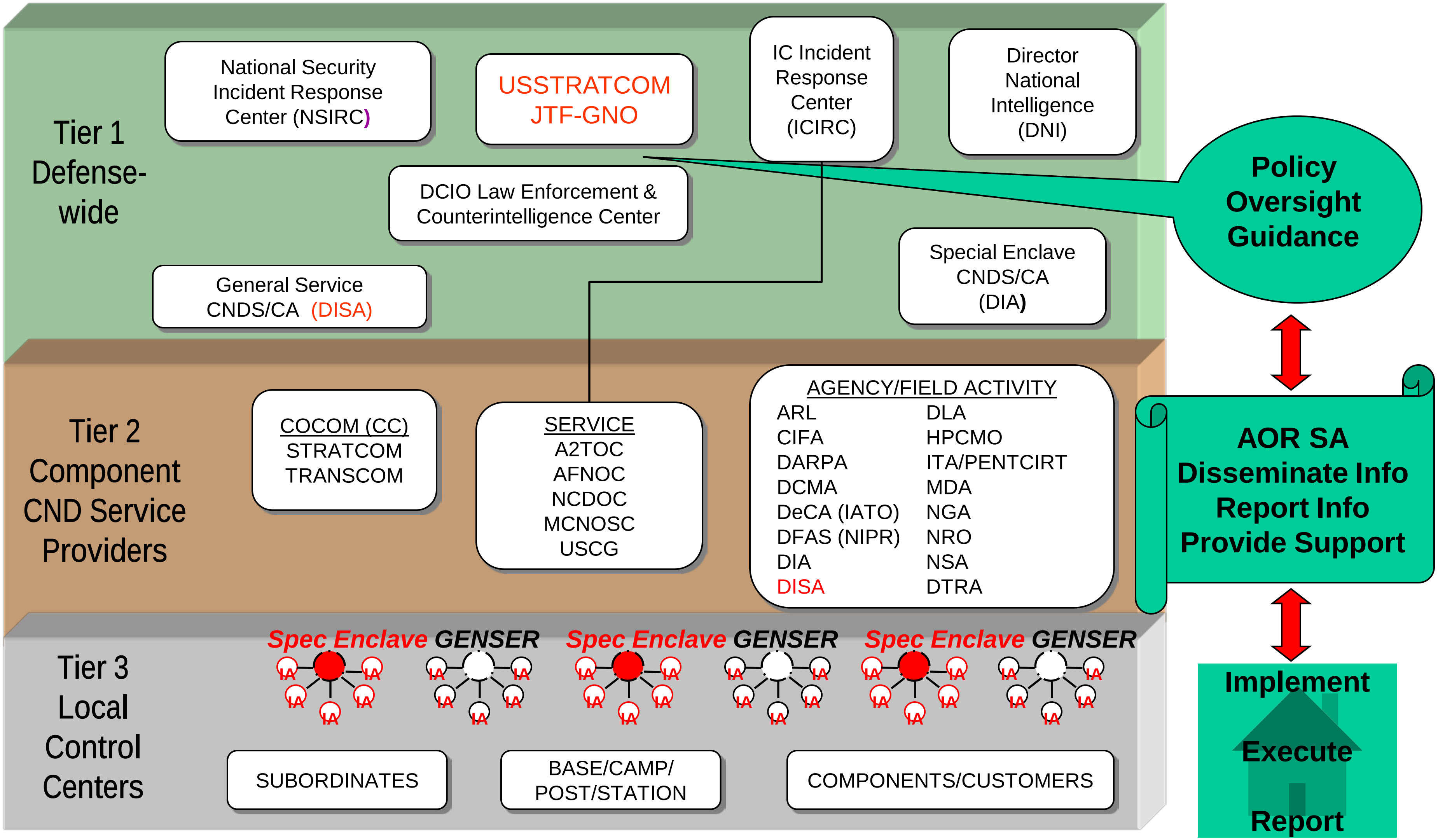
- Origins of IA Requirements
  - U.S. Law
  - JCIDS
  - DoD 8500 series
  - DoD 4630 series
  - DoDAF
  - IT/NSS Interoperability
  - CNDSP

- No Overarching Policy View
- IA policy duplicated
- IA and Computer Network Defense Policies are distinct and interdependent

Consolidation and Clarification is needed!

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Background: IA Performance Dependent Upon Computer Network Defense Providers



Tier 1 Defense-wide

National Security Incident Response Center (NSIRC)

USSTRATCOM JTF-GNO

IC Incident Response Center (ICIRC)

Director National Intelligence (DNI)

DCIO Law Enforcement & Counterintelligence Center

General Service CNDS/CA (DISA)

Special Enclave CNDS/CA (DIA)

Policy Oversight Guidance

Tier 2 Component CND Service Providers

COCOM (CC)
STRATCOM
TRANSCOM

SERVICE
A2TOC
AFNOC
NCDOC
MCNOSC
USCG

AGENCY/FIELD ACTIVITY

ARL	DLA
CIFA	HPCMO
DARPA	ITA/PENTCIRT
DCMA	MDA
DeCA (IATO)	NGA
DFAS (NIPR)	NRO
DIA	NSA
DISA	DTRA

AOR SA
Disseminate Info
Report Info
Provide Support

Tier 3 Local Control Centers

Spec Enclave *GENSER* *Spec Enclave* *GENSER* *Spec Enclave* *GENSER*

SUBORDINATES

BASE/CAMP/POST/STATION

COMPONENTS/CUSTOMERS

Implement

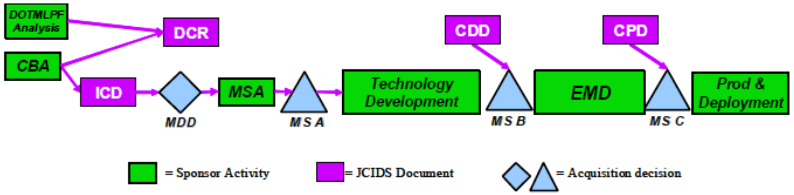
Execute

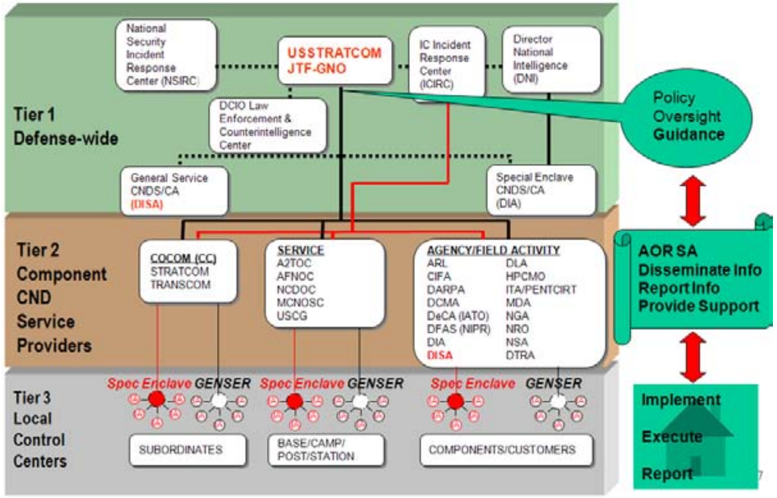
Report

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

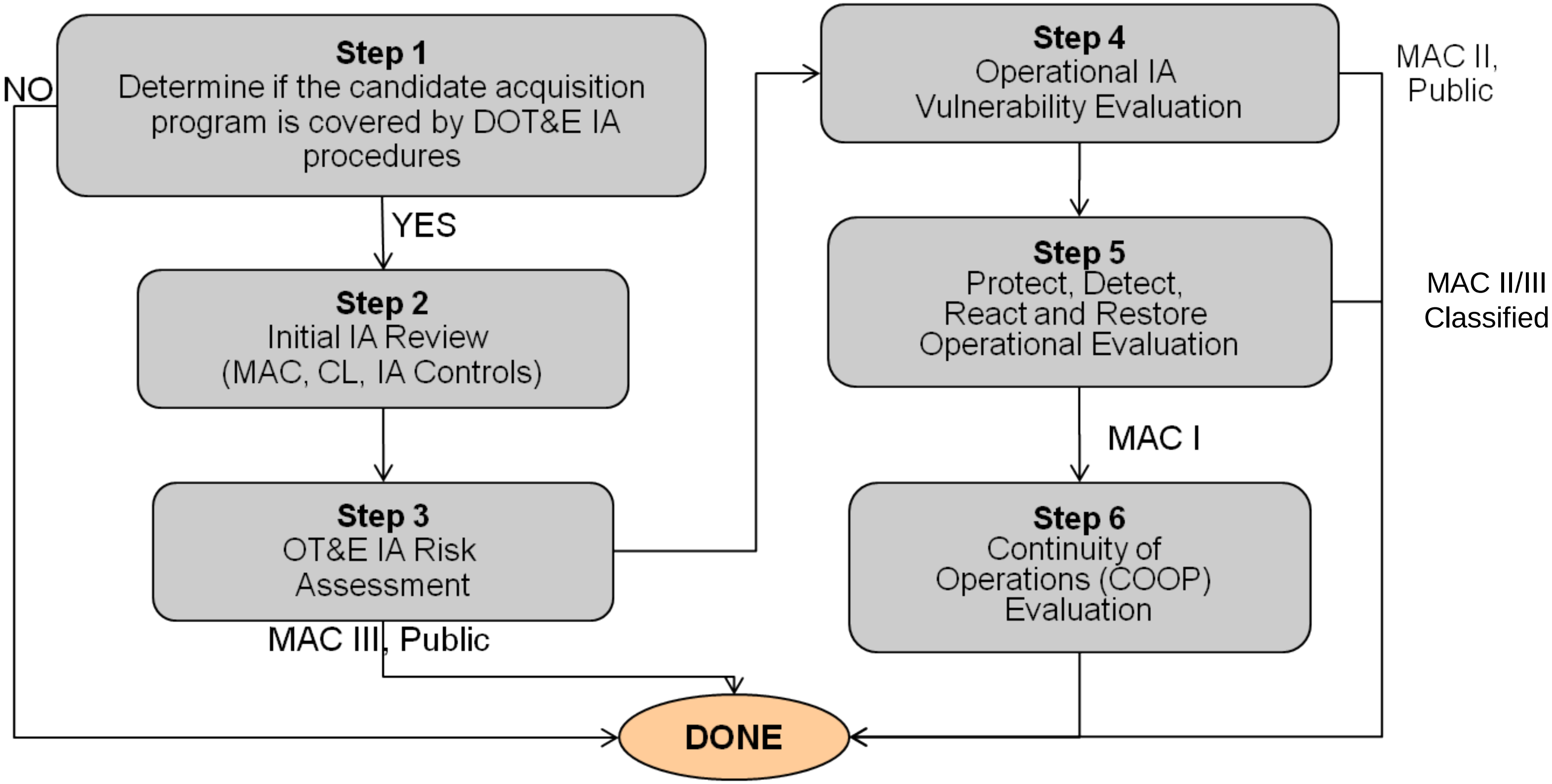
Recommendations: Policy & Guidance

- **CJCSI 3170 JCIDS and CJCSI 6212:**
  - Capabilities must document MAC, CL and CND Service Providers to Identify Interdependencies
- **CJCSI 6212 and DoD 4630**:
  - Solution Architectures must Identify interfaces with CNDSPs
- **DoD 8530 CND Policy**:
  - Establish performance baseline and mandate metrics/testing





Background: DOT&E Six Step Process

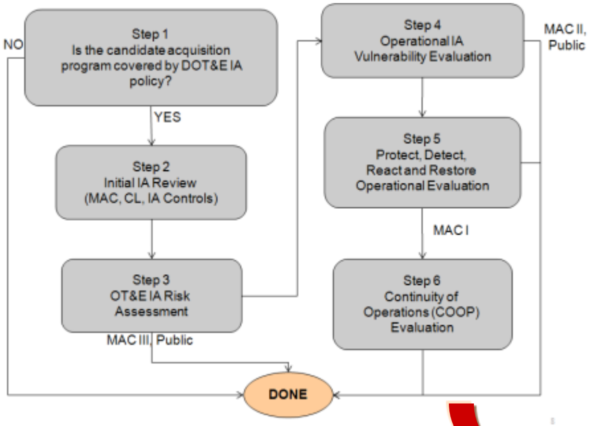

NO
Step 1
Determine if the candidate acquisition program is covered by DOT&E IA procedures
YES
Step 2
Initial IA Review
(MAC, CL, IA Controls)
Step 3
OT&E IA Risk Assessment
MAC III, Public
Step 4
Operational IA Vulnerability Evaluation
MAC II, Public
Step 5
Protect, Detect, React and Restore Operational Evaluation
MAC II/III Classified
MAC I
Step 6
Continuity of Operations (COOP) Evaluation
DONE

DOT&E Process Evaluates IA Operational Effectiveness (MOEs) in a Relevant Operational Environment

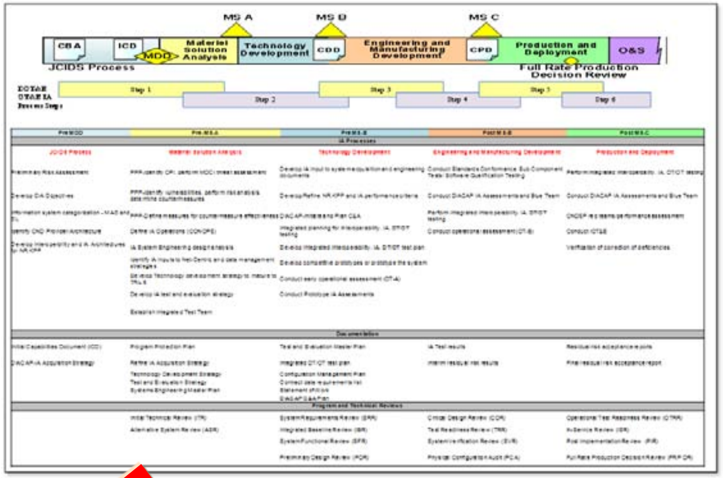
Approved for Public Release; Distribution Unlimited Case Number 10-4034

Recommendations: Policy & Guidance

- DODD 5000.02: Should describe the full-spectrum IA/CND process and
  - Make IA integral to acquisition, systems engineering reviews and milestone entrance/exit criteria
  - Insert DOT&E IA OT Guidance into relevant sections



Step 1
Is the candidate acquisition program covered by DOT&E IA policy?
NO
YES
Step 2
Initial IA Review
(MAC, CL, IA Controls)
Step 3
OT&E IA Risk Assessment
MAC III, Public
Step 4
Operational IA Vulnerability Evaluation
MAC II, Public
Step 5
Protect, Detect, React and Restore Operational Evaluation
MAC I
Step 6
Continuity of Operations (COOP) Evaluation
DONE

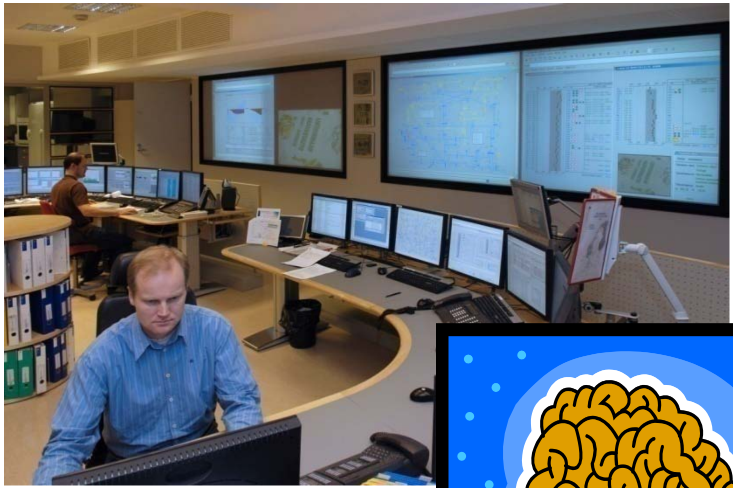


MS A
MS B
MS C
CBA
ICD
MDD
Materiel Solution Analysis
Technology Development
CDD
Engineering and Manufacturing Development
CPD
Production and Deployment
O&S
JCIDS Process
Full Rate Production Decision Review
DOT&E OT&E IA Process Steps
Step 1
Step 2
Step 3
Step 4
Step 5
Step 6
IA Processes
JCIDS Process
Materiel Solution Analysis
Technology Development
Engineering and Manufacturing Development
Production and Deployment
Documentation

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Issue: Acquisition Workforce Training

- **DODD 8570.1 Information Assurance Training, Certification and Workforce Management Policy**
  - Emphasizes network certification and operations
  - Does not address acquisition and T&E processes
- **Acquisition and T&E Work Force lacks critical IA skills**
  - Acquisition, T&E and IA Professionals must cross train
  - Understand threat exposure and mitigation activities



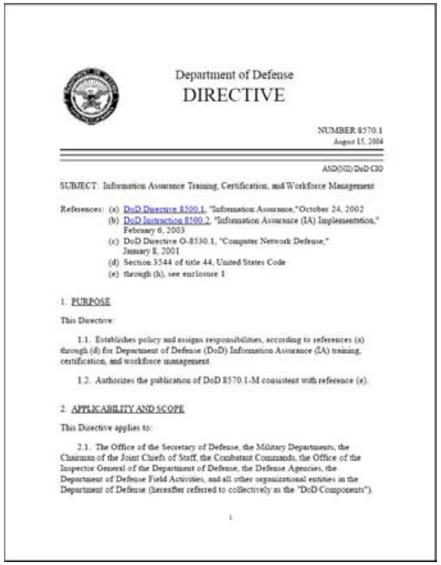
Workforce needs more people who think like the Enemy!

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Recommendations: Training

- **Review DoD 8570.1 and DOD IA Training Curricula to identify gaps**
  - Address needed skills
    - IA Acquisition
    - IA Systems Engineering
    - Integrated IA T&E

- **Supplement in-house knowledge with IA SMEs from industry and academia**
  - Ethical hacking skills needed to
    - Understand potential attack vectors
    - Develop defensive mindset



Department of Defense
DIRECTIVE

NUMBER 8570.1
August 15, 2004

ASD(NII)/DoD CIO

SUBJECT: Information Assurance Training, Certification, and Workforce Management

References: (a) DoD Directive 8500.1, "Information Assurance," October 24, 2002
(b) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(c) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001
(d) Section 3544 of title 44, United States Code
(e) through (h), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities, according to references (a) through (d) for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.

1.2. Authorizes the publication of DoD 8570.1-M consistent with reference (e).

2. APPLICABILITY AND SCOPE

This Directive applies to:

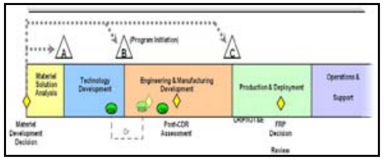
2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the Department of Defense Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

1

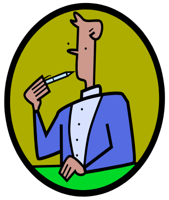
Issue: Requirements Definition, Systems Engineering and Process Execution

IA MOPs/MOEs not adequately addressed in RFP, Contracts and/or Design Reviews

DoD 5000

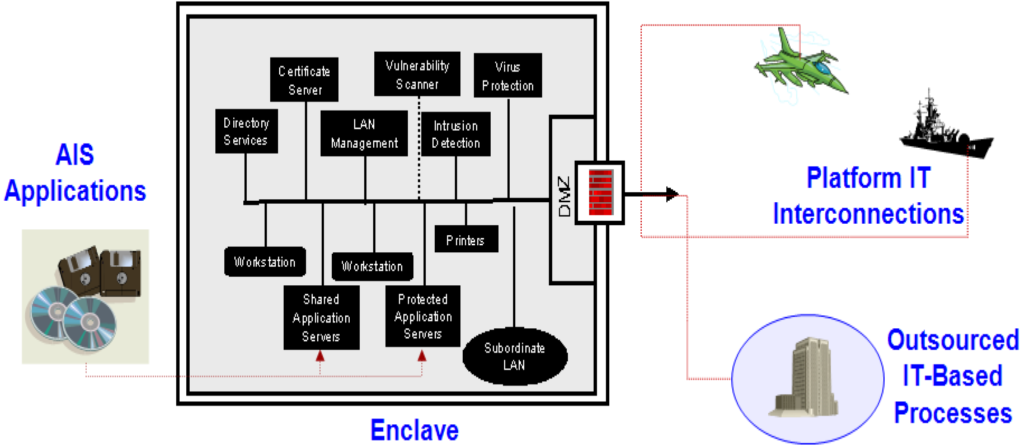


Think IA

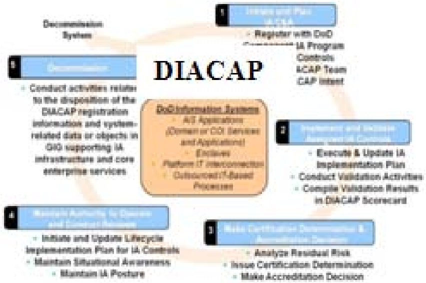


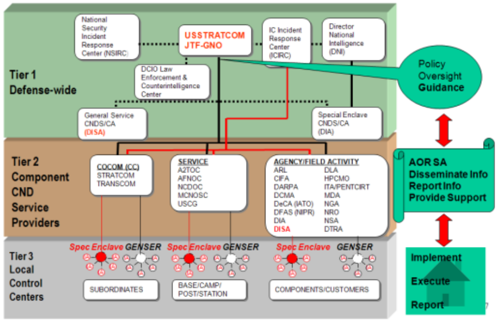
PDR/CDR

IA and CND controls requirements and inheritance not understood



IA Technical Performance and Operational Effectiveness dependent upon CND Inherited Controls


DIACAP
Decommission System
1
Register with DoD
IA Program
Controls
ACAP Team
CAP Intent
2
Execute & Update IA Implementation Plan
Conduct Validation Activities
Compile Validation Results in DIACAP Scorecard
3
Analyze Residual Risk
Issue Certification Determination
Make Accreditation Decision
4
Initiate and Update Lifecycle Implementation Plan for IA Controls
Maintain Situational Awareness
Maintain IA Posture
5
Conduct activities related to the disposition of the DIACAP registration information and system-related data or objects in GIG supporting IA infrastructure and core enterprise services
DoD Information Systems
AIS Applications (Common or COI Services and Applications)
Enclaves
Platform IT Interconnection
Outsourced IT-Based Processes



IA and CND Controls Collectively Contribute to IA Operational Effectiveness

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Integrated Product Team (IPT) vs Integrated Test Team (ITT)

Integrated Product Team (IPT)

- **PM invites representatives from:**
  - DT&E, OT&E IA/CND Testers
  - CNDSP/Local Enclave
  - System Developers
  - System Stakeholders

Collaboration Needed Between ITT and IA IPT

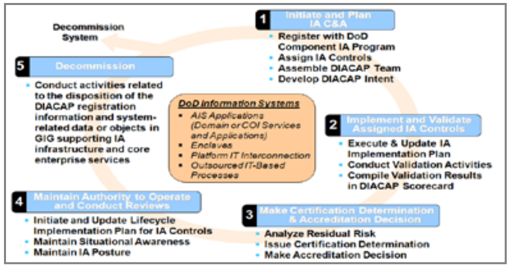
Integrated Test Team (ITT)

- IA/Security/CND Testers
- Interoperability Testers
- Developmental Testers
- Operational Testers

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

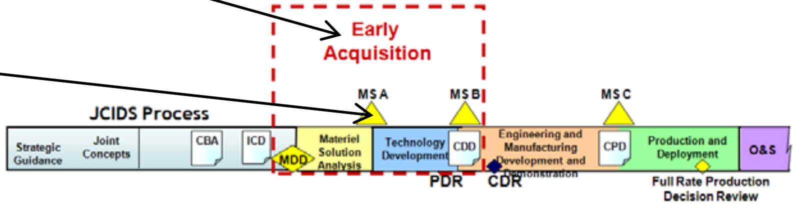
Recommendations: Process Execution Establish Integrated Teams Early (cont.)

- **Establish IA IPT prior to RFP/Contracts**
  - Include DT&E, C&A, OT&E IA and CND testers, PM, system developer, and CNDSP



Decommission System
1 Initiate and Plan IA C&A
Register with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Develop DIACAP Intent
2 Implement and Validate Assigned IA Controls
Execute & Update IA Implementation Plan
Conduct Validation Activities
Compile Validation Results in DIACAP Scorecard
3 Make Certification Determination & Accreditation Decision
Analyze Residual Risk
Issue Certification Determination
Make Accreditation Decision
4 Maintain Authority to Operate and Conduct Reviews
Initiate and Update Lifecycle Implementation Plan for IA Controls
Maintain Situational Awareness
Maintain IA Posture
5 Decommission
Conduct activities related to the disposition of the DIACAP registration information and system-related data or objects in GIG supporting IA infrastructure and core enterprise services
DoD Information Systems
AIS Applications (Domain or COI Services and Applications)
Enclaves
Platform IT Interconnection
Outsourced IT-Based Processes

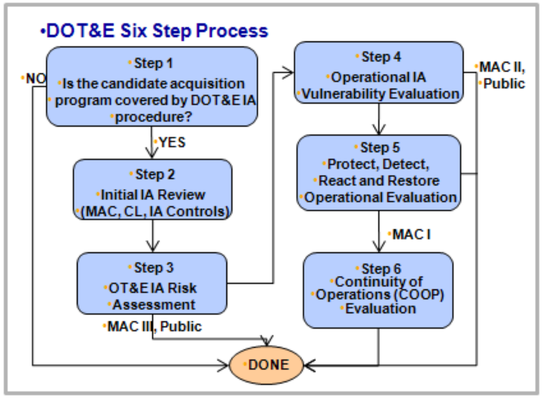
- **Address IA during Early Systems Acquisition/Engineering**



Early Acquisition
JCIDS Process
MS A
MS B
MS C
Strategic Guidance
Joint Concepts
CBA
ICD
MDD
Materiel Solution Analysis
Technology Development
CDD
Engineering and Manufacturing Development and Demonstration
CPD
Production and Deployment
O&S
PDR
CDR
Full Rate Production Decision Review

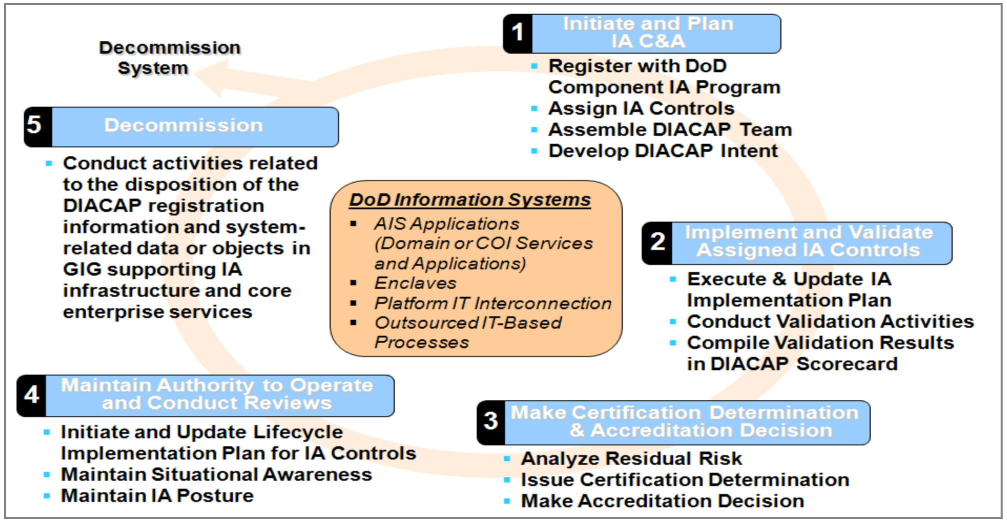
- **Integrated Product Teams (IPT)**
  - Inject IA into Contracts, SE Process, Program and Technical Reviews
    - Translate IA Requirements into Systems Specs
    - Participate in RFP, Source Selection and Contracts
    - Participate in Design and SETRs

- **Integrated Test Teams (ITT)**
  - Collaborate to Identify meaningful/measurable test criteria
    - IA and CND test criteria should address MOP and MOEs
    - Address the End to End IA MOEs as suggested in DOT&E Guidance
  - Critical to “test by one, accept by many.”



DOT&E Six Step Process
NO
Step 1
Is the candidate acquisition program covered by DOT&E IA procedure?
YES
Step 2
Initial IA Review (MAC, CL, IA Controls)
Step 3
OT&E IA Risk Assessment
MAC III, Public
Step 4
Operational IA Vulnerability Evaluation
MAC II, Public
Step 5
Protect, Detect, React and Restore Operational Evaluation
MAC I
Step 6
Continuity of Operations (COOP) Evaluation
DONE

DIACAP Verification vs. DOT&E Validation



Decommission System

5 Decommission
- Conduct activities related to the disposition of the DIACAP registration information and system-related data or objects in GIG supporting IA infrastructure and core enterprise services

1 Initiate and Plan IA C&A
- Register with DoD Component IA Program
- Assign IA Controls
- Assemble DIACAP Team
- Develop DIACAP Intent

DoD Information Systems
- *AIS Applications (Domain or COI Services and Applications)*
- *Enclaves*
- *Platform IT Interconnection*
- *Outsourced IT-Based Processes*

2 Implement and Validate Assigned IA Controls
- Execute & Update IA Implementation Plan
- Conduct Validation Activities
- Compile Validation Results in DIACAP Scorecard

4 Maintain Authority to Operate and Conduct Reviews
- Initiate and Update Lifecycle Implementation Plan for IA Controls
- Maintain Situational Awareness
- Maintain IA Posture

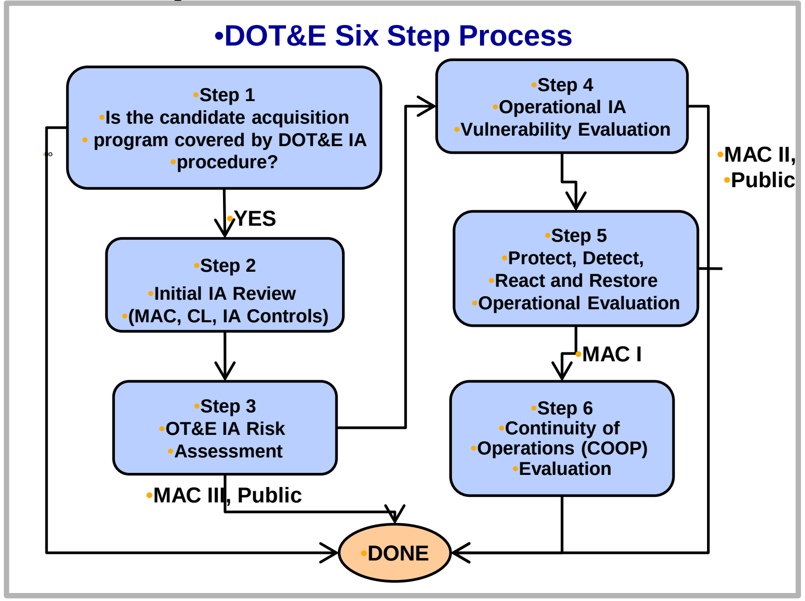
3 Make Certification Determination & Accreditation Decision
- Analyze Residual Risk
- Issue Certification Determination
- Make Accreditation Decision

DIACAP Process –

- IA Controls Verification
  - Standard DOD process
  - Manages IA posture across DOD information systems consistent with FISMA
- Ensures compliance with IA component of the GIG

DOT&E Six Step Process –

- Validates IA Operational Effectiveness
  - Do IA capabilities support the DOD system's effectiveness, suitability, survivability & mission accomplishment?



•DOT&E Six Step Process

•Step 1 •Is the candidate acquisition program covered by DOT&E IA •procedure?

•YES

•Step 2 •Initial IA Review •(MAC, CL, IA Controls)

•Step 3 •OT&E IA Risk •Assessment

•MAC III, Public

•Step 4 •Operational IA •Vulnerability Evaluation

•MAC II, •Public

•Step 5 •Protect, Detect, •React and Restore •Operational Evaluation

•MAC I

•Step 6 •Continuity of •Operations (COOP) •Evaluation

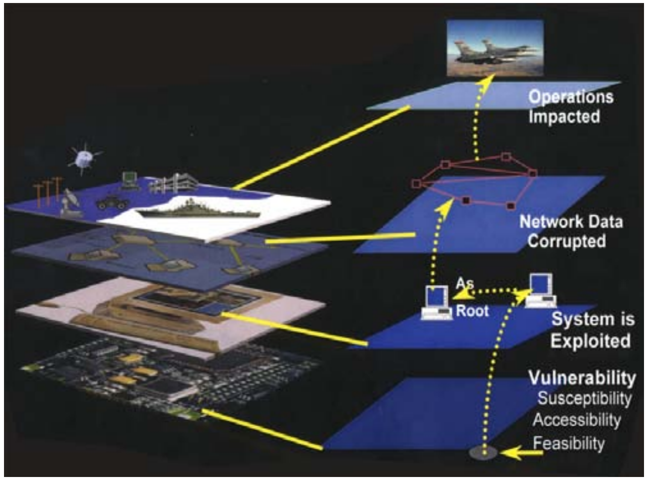
•DONE

DIACAP ATO and IA OT&E not sufficient for fielding – ATC also required

Approved for Public Release; Distribution Unlimited Case Number 10-4034

Recommendations: Process Execution IA Testing

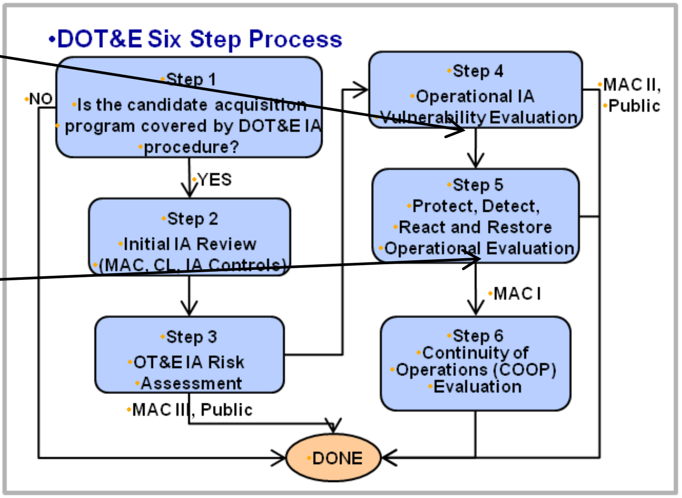
- ATC process not uniform across Services and Components
  - DOD CIO Reciprocity Memorandum Step Forward
  - Incorporate into DOD/Service Policy



- Refine DOT&E 6 Step Process

- DOT&E Step 4:
  - MOP Verification
    - Relevant environments with representative threats
  - Follow with penetration tests
  - Fix technical IA/CND issues before operational assessments

- DOT&E Step 5:
  - MOE Validation
    - Penetration/Exploitation testing for system under test



•DOT&E Six Step Process

Step 1
Is the candidate acquisition program covered by DOT&E IA procedure?

NO

YES

Step 2
Initial IA Review
(MAC, CL, IA Controls)

Step 3
OT&E IA Risk Assessment

MAC III, Public

Step 4
Operational IA Vulnerability Evaluation

MAC II, Public

Step 5
Protect, Detect, React and Restore Operational Evaluation

MAC I

Step 6
Continuity of Operations (COOP) Evaluation

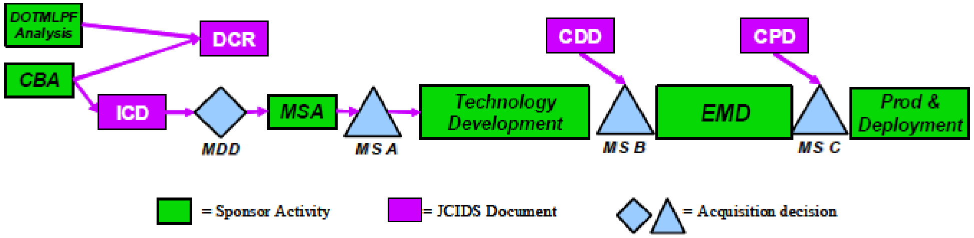
DONE

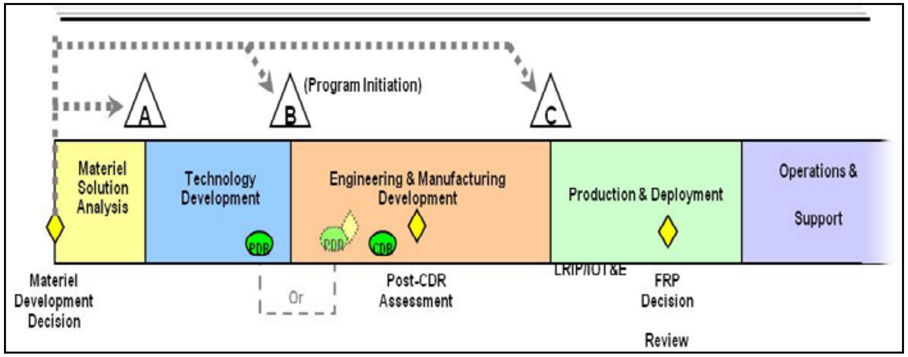
Approved for Public Release; Distribution Unlimited Case Number 10-4034

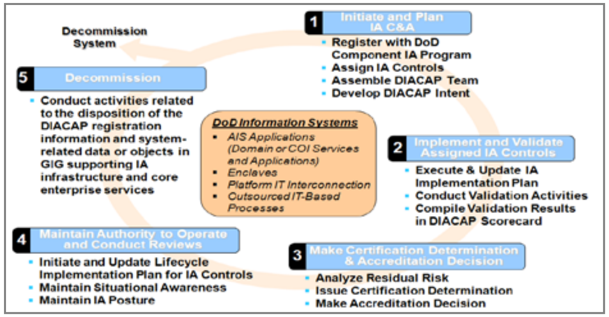
Issue: Requirements Definition, Systems Engineering and Process Execution

- **JCIDS, DOD Acquisition, DOD IA and OSD Testing Policy and Guidance**
  - Coordinated in theory but not in practice

> "In theory, theory and practice are the same…in practice they are not……."
> Yogi Berra







1 Initiate and Plan IA C&A
- Register with DoD Component IA Program
- Assign IA Controls
- Assemble DIACAP Team
- Develop DIACAP Intent

2 Implement and Validate Assigned IA Controls
- Execute & Update IA Implementation Plan
- Conduct Validation Activities
- Compile Validation Results in DIACAP Scorecard

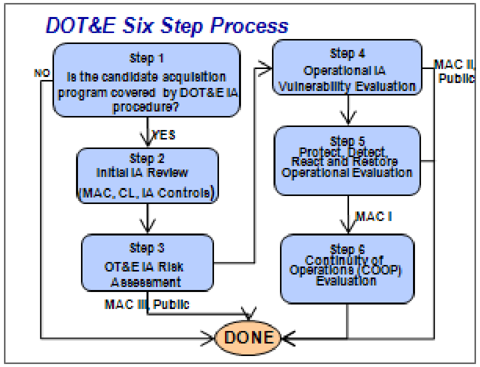
3 Make Certification Determination & Accreditation Decision
- Analyze Residual Risk
- Issue Certification Determination
- Make Accreditation Decision

4 Maintain Authority to Operate and Conduct Reviews
- Initiate and Update Lifecycle Implementation Plan for IA Controls
- Maintain Situational Awareness
- Maintain IA Posture

5 Decommission
- Conduct activities related to the disposition of the DIACAP registration information and system-related data or objects in GIG supporting IA infrastructure and core enterprise services

DoD Information Systems
- *AIS Applications (Domain or COI Services and Applications)*
- *Enclaves*
- *Platform IT Interconnection*
- *Outsourced IT-Based Processes*

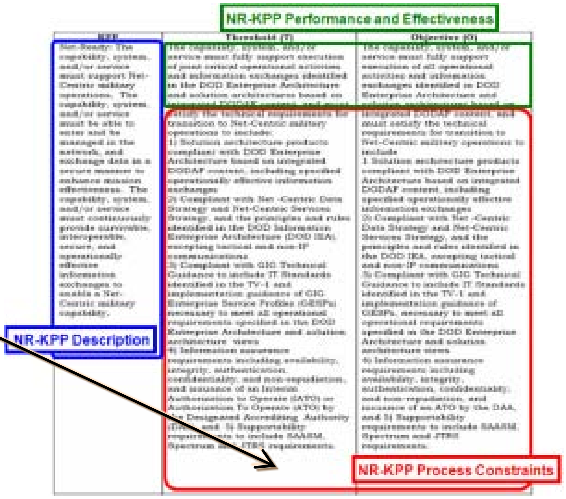
DOT&E Six Step Process


Step 1
Is the candidate acquisition program covered by DOT&E IA procedure?
NO
YES
Step 2
Initial IA Review
(MAC, CL, IA Controls)
Step 3
OT&E IA Risk Assessment
MAC III, Public
Step 4
Operational IA Vulnerability Evaluation
MAC II, Public
Step 5
Protect, Detect, React and Restore Operational Evaluation
MAC I
Step 6
Continuity of Operations (COOP) Evaluation
DONE

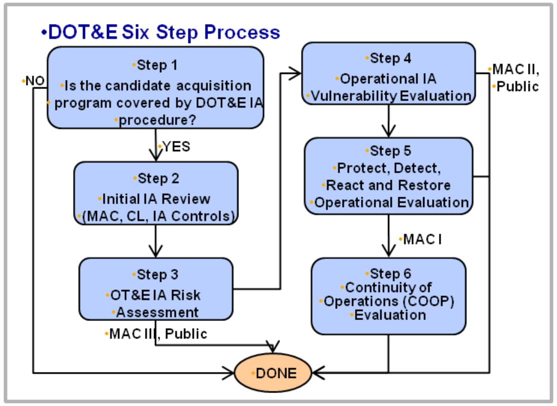
JCIDS, Acquisition, and IA policies are voluminous, difficult to understand and execute!

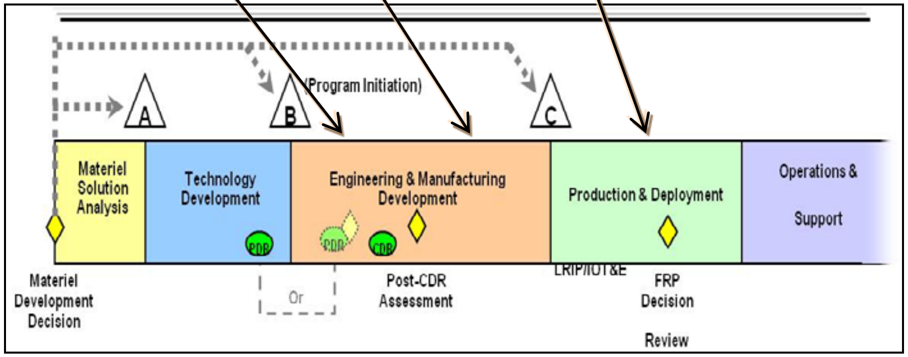
Recommendations: Requirements Definition, Systems Engineering and Process Execution

- Update NR-KPP to address
  - MAC, CL and CNDSP
- Update DOT&E IA OT MOPs
  - Protect, Detect, React, Restore (PDRR) measures
- Inform MDA of IA test findings
  - DT&E, C&A, and OT&E


NR-KPP Performance and Effectiveness

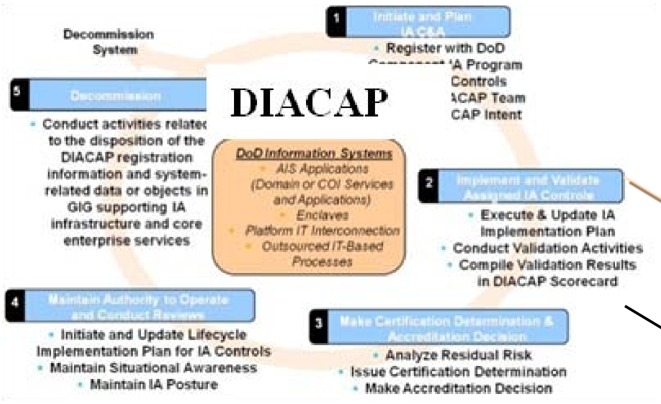
KPP	Threshold (T)	Objective (O)
Net-Ready: The capability, system, and/or service must support Net-Centric military operations. The capability, system, and/or service must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The capability, system, and/or service must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.	The capability, system, and/or service must fully support execution of joint critical operational activities and information exchanges identified in the DOD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1) Solution architecture products compliant with DOD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net -Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DOD Information Enterprise Architecture (DOD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DOD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization To Operate (ATO) by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.	The capability, system, and/or service must fully support execution of all operational activities and information exchanges identified in DOD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include 1 Solution architecture products compliant with DOD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net -Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DOD IEA, excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GESPs, necessary to meet all operational requirements specified in the DOD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an ATO by the DAA, and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.


•DOT&E Six Step Process



Issue: Connected Platform IT

DoD policies for dealing with platform IT are not clearly articulated


DIACAP
Decommission System
1 Initiate and Plan IA C&A
2 Implement and Validate Assigned IA Controls
3 Make Certification Determination & Accreditation Decision
4 Maintain Authority to Operate and Conduct Reviews
5 Decommission

- Register with DoD Component IA Program
- Controls
- ACAP Team
- CAP Intent

DoD Information Systems
- AIS Applications (Domain or COI Services and Applications)
- Enclaves
- Platform IT Interconnection
- Outsourced IT-Based Processes

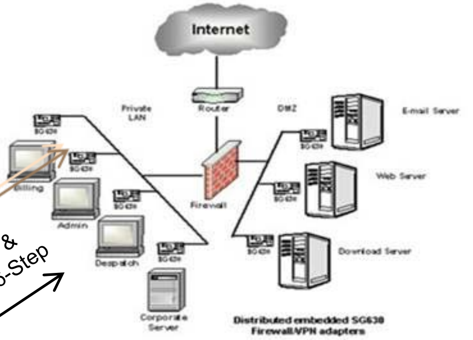
- Execute & Update IA Implementation Plan
- Conduct Validation Activities
- Compile Validation Results in DIACAP Scorecard

- Analyze Residual Risk
- Issue Certification Determination
- Make Accreditation Decision

- Initiate and Update Lifecycle Implementation Plan for IA Controls
- Maintain Situational Awareness
- Maintain IA Posture

- Conduct activities related to the disposition of the DIACAP registration information and system-related data or objects in GIG supporting IA infrastructure and core enterprise services

Conventional IT & NSS



Distributed embedded SG630 Firewall/VPN adapters

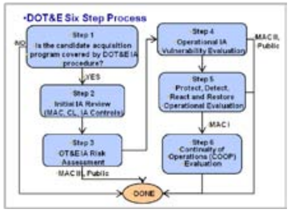
DIACAP &
DOT&E 6-Step

Platform IT?

PIT C&A

Process

PIT Process &
DOT&E 6-step



•DOT&E Six Step Process

Step 1 Is the candidate acquisition program covered by DOT&E IA procedure?
NO → DONE
YES ↓

Step 2 Initial IA Review (MAC, CL, IA Controls)

Step 3 OT&E IA Risk Assessment
MAC III, Public → DONE

Step 4 Operational IA Vulnerability Evaluation
MAC II, Public → DONE

Step 5 Protect, Detect, React and Restore Operational Evaluation
MAC I ↓

Step 6 Continuity of Operations (COOP) Evaluation → DONE

http://www.navy.mil/view_single.asp?id=92493

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

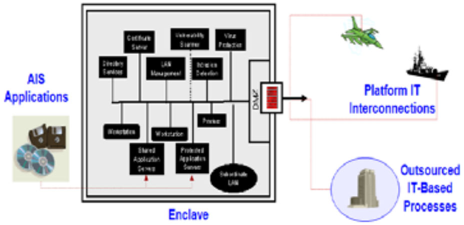
Recommendations: Platform IT

- Clarify PIT Policy without interconnection
  - **Exempt from DIACAP but not from IA**
  - **DODD 5000.01**
    - Clarify requirement to address PIT IA and C&A
  - **DoD 8500**
    - Identify responsible authority for PIT determination
    - Establish PIT criteria for
      - **MAC and CL Assignment**
      - **Minimum PIT IA Controls**
      - **PIT certification process**
  - **CJCSI 6212**
    - Explicitly address PIT and PIT interconnections

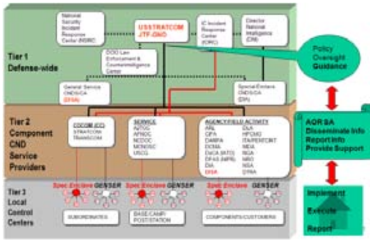
Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Issue: Contracting

- **IA Requirements may**
  - Be omitted in contract or
  - Partially addressed
    - Does not address CNDSP and inherited controls



- **Program Managers need "Acquisition Trained" IA SME's to**
  - Coordinate IA Contracting Requirements
  - Address program vulnerabilities throughout development
  - Lead decisive/early action to mitigate risks

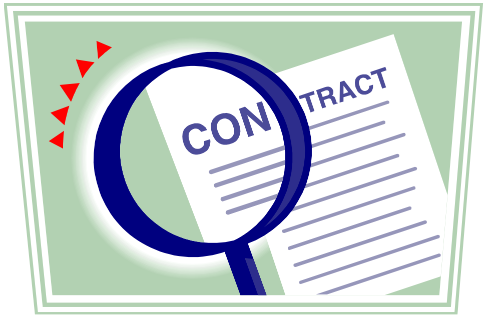

USSTRATCOM JTF-GNO
Tier 1 Defense-wide
Tier 2 Component CND Service Providers
Tier 3 Local Control Centers
Policy Oversight Guidance
AOR SA Disseminate Info Report Info Provide Support
Implement
Execute
Report

Important IA requirements often are omitted in contracts

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Recommendations: Contracting

- **Include measureable and meaningful IA and CND requirements in contracts**
  - RFP SOWs
  - IA technical and operational requirements and CDRLS
  - Address Supply Chain Risk Management (SCRM)
  - Require IA reviews during SFR, PDR, CDR, and support to Integrated Test Teams



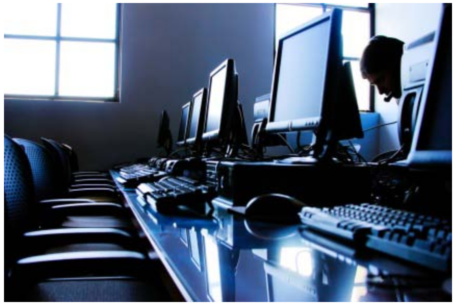
- **Augment contracting staff with IA SMEs for**
  - RFP development
  - Source selection
  - Contract negotiations and monitoring

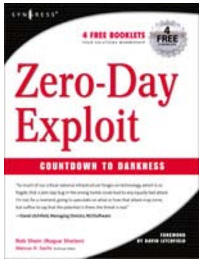
Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Issue: Test Environments/Resources

- **IA Threats constantly change & morph**
  - Threat environment must be continuously reviewed and updated

- **Realistic IA Testing requires**
  - Realistic threat portrayal using network attack/exploitation TTPs
    - *Current* threat environment
  - Penetration & Exploitation testing
    - Satisfies Developer, C&A and OT&E test requirements for acquisitions





4 FREE BOOKLETS

FREE

Zero-Day Exploit

COUNTDOWN TO DARKNESS

Cyber Warfare

Cyber Crime

Cyber Espionage

Current, representative threats needed for acquisition T&E activities

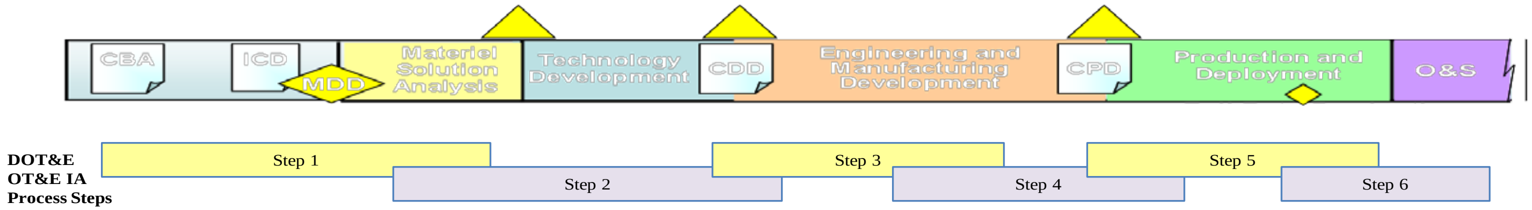
Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Recommendations: Test Environment and Resources

- Update DODD 8500.1, DODI 5000.02 and DAG
  - Make Acquisition related IA and CND T&E a priority
    - Helps to ensure security of DOD systems
- Intelligence Community
  - Provide up-to-date threat characterization information available to the acquisition T&E community
- Service Components
  - Develop/resource IA and CND Acquisition T&E capabilities to execute penetration testing for OT&E
- Acquisition T&E community
  - Ensure that DOT&E Step 5 IA/CND "Effectiveness" testing is performed in relevant operational environments
- JS, DDT&E and DOT&E
  - Mature IA Cross Walk "Proposed Framework" for integrated IA and CND Acquisition, Test and Evaluation

IA and CND testing in acquisition is a *critical activity and can only* be accomplished with adequate resources and threat characterization

Proposed Framework for Joint, Integrated IA and CND Acquisition, Test and Evaluation


CBA
ICD
MDD
Materiel Solution Analysis
Technology Development
CDD
Engineering and Manufacturing Development
CPD
Production and Deployment
O&S
DOT&E OT&E IA Process Steps
Step 1
Step 2
Step 3
Step 4
Step 5
Step 6

Pre MDD	Pre-MS-A	Pre MS-B	Post MS-B	Post MS-C
IA Processes				
JCIDS Process	**Materiel Solution Analysis**	**Technology Development**	**Engineering and Manufacturing Development**	**Production and Deployment**
Preliminary Risk Assessment	PPP-Identify CPI, perform MDCI threat assessment	Develop IA input to system acquisition and engineering documents	Conduct Standards Conformance, Sub Component Tests/ Software Qualification Testing	Perform integrated Interoperbailty, IA, DT/OT testing
Develop CIA Objectives	PPP-Identify vulnerabilities, perform risk analysis, determine countermeasures	Develop/Refine NR KPP and IA performance criteria	Conduct DIACAP IA Assessments and Blue Team	Conduct DIACAP IA Assessments and Blue Team
Information system categorization - MAC and CL	PPP-Define measures for countermeasure effectiveness	DIACAP-Initiate and Plan C&A	Perform integrated Interoperability, IA, DT/OT testing	CNDSP red teams/performance assessment
Identify CND Provider/Architecture	Define IA Operations (CONOPS)	Integrated planning for interoperability, IA, DT/OT testing	Conduct operational assessment (OT-B)	Conduct IOT&E
Develop Interoperbility and IA Architectures for NR KPP	IA System Engineering design analysis	Develop integrated Interoperability, IA, DT/OT test plan		Verification of correction of deficiencies
	Identify IA inputs to Net-Centric and data management strategies	Develop competitive prototypes or prototype the system		
	Develop Technology development strategy to mature to TRL 6	Conduct early operational assessment (OT-A)		
	Develop IA test and evaluation strategy	Conduct Prototype IA Assessments		
	Establish Integrated Test Team			
Documentation				
Initial Capabilities Document (ICD)	Program Protection Plan	Test and Evaluation Master Plan	IA Test results	Residual risk acceptance reports
DIACAP-IA Acquisition Strategy	Refine IA Acquisition Strategy	Integrated DT/OT test plan	Interim residual risk results	Final residual risk acceptance report
	Technology Development Strategy	Configuration Management Plan		
	Test and Evaluation Strategy	Contract data requirements list		
	Systems Engineering Master Plan	Statement of Work		
		DIACAP C&A Plan		
Program and Technical Reviews				
	Initial Technical Review (ITR)	System Requirements Review (SRR)	Critical Design Review (CDR)	Operational Test Readiness Review (OTRR)
	Alternative System Review (ASR)	Integrated Baseline Review (IBR)	Test Readiness Review (TRR)	In-Service Review (ISR)
		System Functional Review (SFR)	System Verification Review (SVR)	Post Implementation Review (PIR)
		Preliminary Design Review (PDR)	Physical Configuration Audit (PCA)	Full Rate Production Decision Review (FRP DR)

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Conclusions

- Address IA Capabilities Earlier and Throughout System Development Lifecycle
- Include IA Requirements and CDRLs in Contracts
- Develop Overarching, Unified IA Requirements, Engineering, and Testing Process
- Form Integrated Test Teams Early
- Promote Acquisition-Related IA and CND T&E as Critical to Ensure Secure DOD Systems

IA must be addressed early and throughout the acquisition lifecycle to ensure successful IA OT&E and a Secure and Resilient DOD Enterprise

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034

Next Steps

- IA Policy Crosswalk WG report has been disseminated to T&E Community
- OSD DOT&E and AT&L DDRE DT are collaborating to update IA OT Policy and Guidance
- AT&L DDT&E and OSD DOT&E
  - Promoting active dialogue with Joint Staff, NII/CIO, AT&L and other DOD Organizations

Questions?

Approved for Public Release;
Distribution Unlimited
Case Number 10-4034