

Information Assurance (IA) Update



IA Policies and Processes

Tuesday, April 20, 2010





Topics

- Information Assurance (IA)
 - What's IA
 - What's Certification & Accreditation
 - IA Compliance
 - IA in Navy Contracts
 - How do we do IA
- DoD IA Implementation & Controls
- NIST Special Publication 800-53A
- DoD Information Assurance Certification and accreditation process (DIACAP)
- DoD Reciprocity Memo
- NIST Releases Special Publication 800-37 Revision 1
- Federal Information Security Management Act (FISMA)
- Information Assurance (IA) Roadmap
- How to help yourself



What's IA

- Measures that protect and defend information and information systems by ensuring their:
 - Availability
 - Timely, reliable access to information
 - Integrity
 - Protection against unauthorized modification of information
 - Authentication
 - Designed to establish the validity of a transmission, message, originator, or an individual's authorization to receive specific information
 - Confidentiality
 - Assurance that information is not disclosed to unauthorized individuals, processes, or devices
 - Non-repudiation
 - Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data
- This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities



What's C&A

- **Certification:** A comprehensive evaluation and validation of a DOD Information System to establish the degree to which it complies with assigned IA controls based on standardized procedures.
- **Accreditation:** A formal statement by a designated accrediting authority (DAA) regarding acceptance of the risk associated with operating an information system and expressed as an authorization to operate (ATO), interim ATO (IATO), interim authorization to test (IATT), or denial of ATO (DATO).



IA in Navy Contracts

- SECNAV M-5239.1 DoN Information Assurance Program; Information Assurance Manual
- National Industrial Security Operating Manual (NISPOM)
- CJCSI 6211.02 (series) --Defense Information System Network (DISN): Policy Responsibilities and Processes of 31 July 2003
- CJCSI 6212.01E (series) --Interoperability and Supportability of Information Technology and National Security Systems
- DoDD 8100.1--Global Information Grid (GIG) Overarching Policy
- DoDD 8500.1E--Information Assurance
- **DoDI 8500.2--Information Assurance Implementation**
- ***DODI 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP), November 28, 2007***
- CNO N614/HQMC C4--Navy-Marine Corps Unclassified Trusted Network Protection (UTN-Protect) Policy, Version 1.0, 31 October 2002”
- DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management, August 15, 2004, Certified Current as of April 23, 2007
- Department of the Navy Chief Information Officer (DON CIO) Memorandum 01-09, Information Assurance Policy for Platform Technology, January 30, 2009
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products
- SECNAVINST 5230.15, Information Management/Information Technology Policy for Fielding of Commercial Off the Shelf Software, April 10, 2009





How do we do IA?

- We assess applicability of DoD IA controls to our systems.
- We determine whether we should avoid, control, accept, or transfer risks for which the IA controls prescribe countermeasures.
 - Risk = Threat x Vulnerability x Cost/Value (of information)
- We implement and validate technical, procedural, and/or administrative countermeasures to eliminate or mitigate risk.
- We draft agreements with organizations from which we inherit or share satisfaction of controls.
- We document and support rationale for retaining risk.



How do we do IA?

- The process of validation confirms and/or establishes by testing, evaluation, examination, investigation, or competent evidence that an information system's assigned IA controls are implemented correctly and are effective in their application.
- Prior to test or fielding of a new system (or making any change to a system that affects its security posture), an accreditation decision is required, so we do some sort of a C&A drill to support it.
 - C&A is NOT IA
 - Involves validation and documentation of due diligence
 - Results in acceptance of risk by a Designated Approving Authority





DoDI 8500.2 - IA Implementation



Department of Defense INSTRUCTION

NUMBER 8500.2

February 6, 2003

ASD(C3I)

SUBJECT: Information Assurance (IA) Implementation

PURPOSE: Implements policy (8500.1), assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks

Establishes a baseline set of IA Controls to be applied to all DoD information systems. Each IA Control is uniquely named and formally catalogued, and can therefore be referenced, measured, and reported against throughout the life cycle of a DoD information system.



8500.2 IA Controls



DoD 8500.2 IA
Control Template



8500.2 IA Controls Almost Gone



DoD 8500.2
Controls Almost Gone



New IA Control Set

NIST Special Publication 800-53A

NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce

Guide for Assessing the Security Controls in Federal Information Systems

Building Effective Security Assessment Plans

Ron Ross
Arnold Johnson
Stu Katzke
Patricia Toth
Gary Stoneburner
George Rogers



DIACAP



Department of Defense **INSTRUCTION**

NUMBER 8510.01
November 28, 2007

ASD(NII)/DoD CIO

SUBJECT: DoD Information Assurance Certification and Accreditation Process (DIACAP)



DIACAP Almost Gone



DEPARTMENT OF DEFENSE
INSTRUCTION

NUMBER 8510.01
September 28, 2007

(NII)/DoD CIO

SUBJECT: DoD Information Systems Security Accreditation and Certification Process (DIACAP)





DoD Reciprocity Memo



DoD PAAs

**DEPARTMENT OF DEFENSE
WASHINGTON, DC 20301**

23 July 2009

MEMORANDUM FOR: SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
COMBATANT COMMANDERS
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

Subject: DoD Information System Certification and Accreditation Reciprocity

This memorandum defines reciprocity as:

“mutual agreement among participating enterprises to accept each other's security assessments in order to reuse IS resources and/ or accept each other's assessed security posture in order to share information.”



Not Reciprocity



DoD PAAs

MEMORANDUM

SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
COMBATANT COMMANDERS
UNDER SECRETARIES OF DEFENSE
REPUBLICAN MANAGEMENT CENTER
SECRETARIES OF DEFENSE
ASSTANTS TO THE SECRETARY OF DEFENSE
OFFICERS OF DEFENSE
ACTIVITIES

July 2009

Subject: DoD Information Security Accreditation Reciprocity

This memorandum defines reciprocity as:

“mutual agreement among participating enterprises to accept each other's security assessments in order to reuse IS resources and/ or accept each other's assessed security posture in order to share information.”



Upcoming C&A Process

NIST Special Publication 800-37
Revision 1

NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce

Guide for Applying the Risk Management Framework to Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

- This publication represents the second in a series of publications being developed to provide a common information security framework for the federal government and its contractors.
- Changes the traditional process employed by the federal government to certify and accredit federal information systems.
- NIST Special Publication 800-37, Revision 1, is the full transformation of the Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF).



FISMA

- Federal Information Security Management Act of 2002 (FISMA)
 - Implement an agency-wide information security program
 - DON CIO is lead for Navy departmental compliance with FISMA
 - The elements of a DOD information system IA program are developed and maintained through the DOD IA Certification & Accreditation (C&A) process

Percentage of Systems with a:	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008
Certification and Accreditation	47%	62%	77%	85%	88%	92%	96%
Tested Contingency Plan	35%	48%	57%	61%	77%	86%	92%
Tested Security Controls	60%	64%	76%	72%	88%	95%	93%
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	10,304	10,679



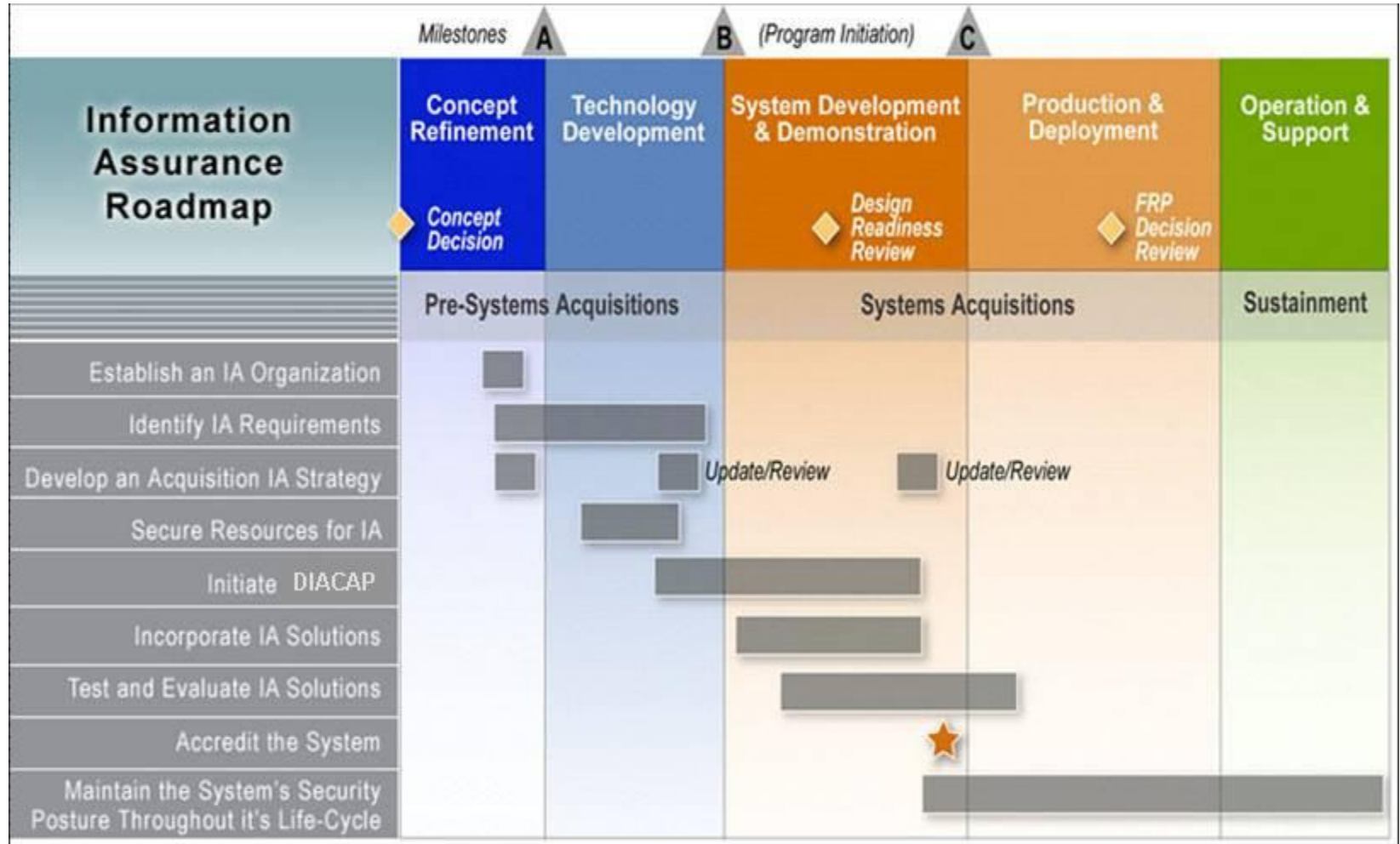
FISMA

Table 4: Results of IG Assessments for Fiscal Year 2008 FISMA annual report

Agency	Effective POA&M ?	Quality of Certification and Accreditation Process	Completeness of System Inventory	Quality of Privacy Impact Assessment Process
Agency for International Development	Yes	Excellent	96-100%	Excellent +
Department of Agriculture	No	Poor	81-95% +	Satisfactory +
Department of Commerce	Yes	Satisfactory +	96-100%	Good
Department of Defense	No	Failing	0	Failing
Department of Education	Yes	Satisfactory	96-100%	Excellent +
Department of Energy	Yes	Satisfactory	96-100%	Satisfactory
Environmental Protection Agency	Yes	Good +	96-100%	Excellent +
General Services Administration	Yes	Satisfactory	96-100%	Satisfactory
Department of Health and Human Services	Yes	Satisfactory -	81-95% -	Good -
Department of Homeland Security	Yes	Good +	96-100%	Good
Department of Housing and Urban Development	Yes	Satisfactory	96-100%	Satisfactory -
Department of the Interior	No	Satisfactory +	96-100%	Excellent +
Department of Justice	Yes	Good -	96-100%	Excellent
Department of Labor	Yes	Satisfactory	96-100%	Good
National Aeronautics and Space Administration	Yes	Excellent +	96-100%	Good
National Science Foundation	Yes	Good	96-100%	Excellent
Nuclear Regulatory Commission	Yes	Satisfactory +	96-100% +	Excellent
Office of Personnel Management	Yes	Satisfactory -	96-100%	Excellent +
Small Business Administration	Yes	Satisfactory	96-100%	Satisfactory
Smithsonian Institution	Yes	Satisfactory	96-100% +	Satisfactory -
Social Security Administration	Yes	Good -	96-100%	Excellent +
Department of State	Yes	Good +	96-100 %	Good +
Department of Transportation	No	Satisfactory	96-100%	Satisfactory -
Department of the Treasury	Yes	Satisfactory	96-100% +	Satisfactory
Department of Veterans Affairs	Yes	Satisfactory +	96-100% +	Satisfactory +



Information Assurance Roadmap





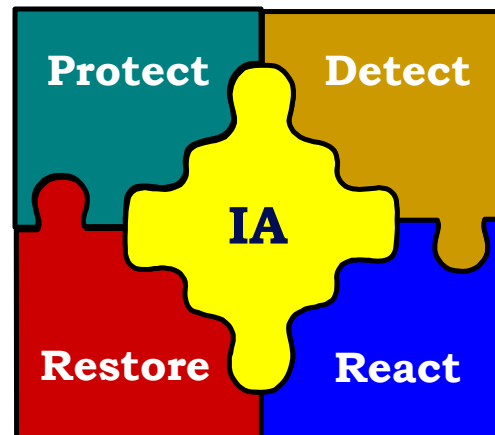
How to Help Yourself

- Train your IA personnel in DoD policy
- Get an IA person on your proposal team
- Employ an IA person during system development
- Utilize Federal Desktop Core Configuration (FDCC) compliant software
- Invest in PKI certificates
 - External Certification Authorities (ECA)
 - DoD Common Access Cards (CAC)



Conclusion

IA has become increasingly important to Joint operations and effective defense system performance. The success of net-centric warfare depends greatly on the implementation of IA



A Risk accepted by ONE is a Risk shared by ALL

Questions?





Contact

Christopher Dosch
NAVAIR PMA260 IA Support
(c) 703-408-6399
christopher.dosch.ctr@navy.mil