



# Department of Defense Information Assurance Policy and Implementation



# Today's Climate

- DoD operates in a highly interactive environment of interconnected applications and services across global networks using powerful computing devices.
- DoD Components routinely interact with the governments of other nations, coalition partners, other U.S. government agencies, commercial partners, and research partners.
- The complexity of today's systems and networks presents **significant security challenges** for both producers and consumers of information technology.



# What is Information Assurance?

Information Assurance (IA) is defined as measures that **protect** and **defend** information and information systems by ensuring their **availability, integrity, authentication, confidentiality, and non-repudiation**. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.



# DoD Information Assurance Goals

The DoD Information Assurance Strategy and Roadmap for addressing security in today's climate includes the following five goals.

1. Provide end-to-end protection of DoD information.
2. Defend DoD information systems and computer networks from unauthorized or malicious activity.
3. Provide information assurance (IA) situational awareness and command and control (C2).
4. Improve IA processes through integration.
5. Create an empowered IA workforce.



# DoD IA Policy Framework

To meet its IA goals, the Department of Defense is developing a comprehensive framework of IA policy. DoD Directive 8500.1 and DoD Instruction 8500.2 are the “capstone” policy documents that lay the foundation for the framework, illustrated below.

<b>IA Goal</b>	<b>Policy Series</b>	<b>Policy Subject Area</b>
ALL	8500	General
ALL	8510	IA Certification and Accreditation
1,3	8520	Security Management
2	8530	Computer Network Defense
1	8540	Interconnectivity
1,2,3	8550	Network and Web
1,2,3	8560	IA Monitoring
5	8570	IA Education, Training, and Awareness
4	8580	Other (Integration)



# The DoD IA Program

DoDI 8500.2 defines a three-level DoD IA Program :

1. The Defense IA Program
2. DoD Component IA Programs
3. Individual DoD Information System IA Programs

The Defense IA Program provides standards and support to the DoD Component IA programs, and delivers Defense-wide IA capabilities. The DoD Component IA Programs provide support to individual DoD information system IA programs and deliver Component-wide IA capabilities. DoD information system IA programs manage IA across the information system life cycle, and provide IA situational awareness to the DoD Component and Defense IA programs.



# The Defense IA Program

The Defense IA program provides:

1. A coordination and integration across all Components
2. DoD IA Controls, nine baseline sets of best security practices and associated compliance metrics that provide pre-established levels of confidentiality, integrity, and availability
3. DoD-wide IA management review and assessment
4. IA Technical Framework
5. A product specification and evaluation framework for IA and IA-enabled IT products
6. Security configuration specifications for IA and IA-enabled products
7. DISN connection management and cross-domain solutions
8. Defense-wide Computer Network Defense
9. A Key Management Infrastructure (KMI) that includes a Public Key Infrastructure (PKI) and an Electronic Key Management System (EKMS)
10. IA Support Services (e.g., the IA Support Environment (IASE) and the IA Technology Analysis Center (IATAC))
11. Courseware for a core curriculum of IA training and awareness



# DoD Component IA Programs

Each DoD Component IA program provides:

1. A Component-level IA architecture / master plan for Component-wide implementation Defense-in-Depth principles of layered protections at the network and infrastructure, the enclave boundaries, and the computing environments
2. Visibility of IA in PPBS
3. Clear delineation of IA roles and responsibilities at all organizational and IT levels
4. Component-level IA education, training and awareness capabilities
5. Mission Assurance Category (MAC) and confidentiality level designation for all Component information systems
6. Integration of IA into IT configuration management programs and processes
7. IA monitoring capability
8. Regular assessment of IA posture through assessments, audits, testing, and program reviews
9. CND Services for all Component information systems



# DoD Information System IA Programs

Each DoD Information System IA program provides:

1. System level protection and detection capabilities that are consistent with the Component-level IA architecture and the DoD IA Controls
2. Documentation of the capabilities and the IA program
3. Access control / authorization for the use of the system hardware and software
4. Integration of IA requirements and management processes into the system's configuration management processes, to include proactive vulnerability management
5. A reporting and response capability for IA violations and incidents
6. Continuity of IT and IA services
7. Tracking, managing, and reporting the system's IA posture, to include IA Controls compliance, IAVA compliance, and other readiness indicators, and the status of Component-level management review items



# DoD Information System IA Programs

## Key IA Protection Requirements

1. Develop and implement an enclave-level IA architecture that incorporates Defense-in-Depth principles of layered protections at the network and infrastructure, the enclave boundary, and the computing environment.
2. Acquire IA and IA-enabled products that meet good IA specifications and have been evaluated by US Government or internationally recognized processes.
3. Configure and deploy IA and IA-enabled products in accordance with established DoD security configuration specifications.
4. Design and build IA services into AIS applications, following established security engineering and software quality principles.
5. Independently validate that the DoD information system provides adequate security, meets DoD requirements for IA C2 and IA readiness, conforms to DoD network ports, protocols, and services standards, and “plugs into” DoD supporting IA infrastructures (IA Certification and Accreditation).



# DoD Information System IA Programs

## Key IA Protection Requirements (continued)

6. Manage interconnection risks by complying with DoD connection management processes.
7. Grant user access in accordance with DoD personnel security requirements.
8. Protect information that transits non-DoD networks and computing environments according to its confidentiality and sensitivity requirements.
9. Maintain a secure enclave and computing environment by proactively assessing for vulnerabilities, applying software patches and upgrades in a timely manner, and complying with the DoD IAVA process.
10. Provide IA awareness training for all authorized users.
11. Train and certify IA and IT professionals in IA roles and responsibilities.



# DoD Information System IA Programs

## Key CND Requirements

1. Ensure that a CND Service Provider for the DoD information system is identified and a documented working interface is established (e.g., an incident response plan).
2. Continuously monitor the DoD information system for unauthorized activity. (See multiple DoD IA Controls in Enclosure 4 of DoDI 8500.2 for system audit requirements).
3. Conduct periodic in-depth monitoring and penetration testing.
4. Provide for system continuity / restoration (e.g., a continuity of operations or disaster recovery plan)

***See DoDD O-8530.1 and DoDI O-8530.2 for CND policy.***



# 4 Categories of DoD Information Systems

To improve IA management accountability, all DoD information systems are organized into four categories:

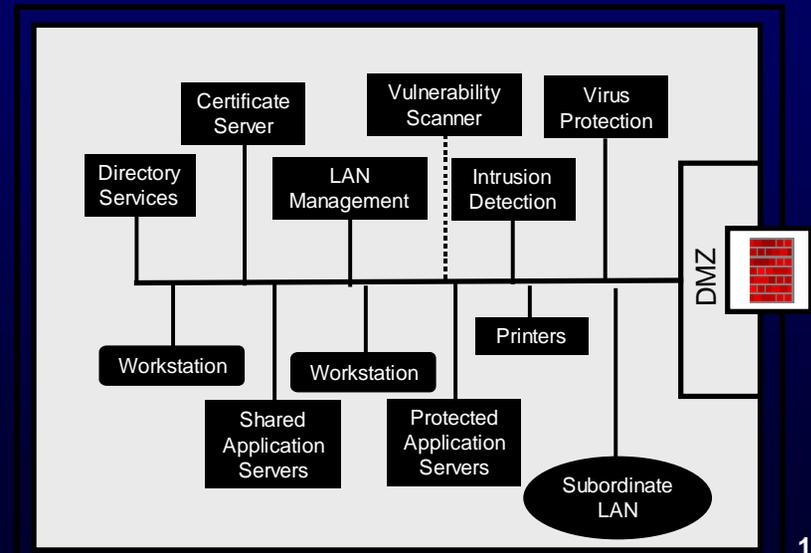
	Category	Primary IA Focus
1	Enclaves (which includes networks)	IA in IT operations
2	AIS Applications	IA in system design and development
3	Outsourced IT-based processes	IA in source selection and service performance parameters, and allocation of procedural security between service provider and government users
4	Platform IT interconnections	Network connection rules and compliance monitoring



# Enclaves

- For DoD IA purposes, an enclave is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.
- Enclaves provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail.
- Enclaves are the interconnecting agent for all other categories of systems.
- Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

## Notional Enclave





# AIS Applications

For DoD IA purposes an AIS Application:

- Is the product or deliverable of an acquisition program (e.g., DoDD 5000.1)
- May be:
  - Single software application (e.g., Integrated Consumable Items Support (ICIS))
  - Multiple software applications related to a single mission (e.g., payroll or personnel)
  - Combination of S/W and H/W performing a specific support function across a range of missions (e.g., GCCS, DMS)
- Performs clearly defined functions for which there are readily identifiable security considerations and needs addressed by the PM as part of the acquisition
- Has a security design that conforms to DoD Component IA architecture and utilizes common IA services provided by enclaves
- Is deployed to enclaves for operations, which assume responsibility for operational security
- Is managed across its life cycle, with the PM responsible for addressing security in new releases



# Outsourced IT-based Processes

For DoD IA purposes, an outsourced IT based process:

- Is a general term used to refer to:
  - Outsourced business processes supported by private sector information systems
  - Outsourced information technologies
  - Outsourced information services
- Is not under DoD configuration control, and is not dedicated to DoD processing or DoD users
- Performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations
  - Technical security is responsibility of the service provider
  - Responsibility for administrative and procedural security is shared between the government and the service provider
  - Security roles and responsibilities are addressed in the acquisition
  - IA posture is assessed via performance and service level parameters which are defined in the acquisition



# Platform IT Interconnection

For DoD information assurance purposes, platform IT interconnection:

- Refers to external network access to platform IT
- Is always with an enclave
- Has readily identifiable security considerations and needs that must be addressed in operations and may need to be addressed in acquisition
  - Platform IT is responsible for IA of information it processes inherent to its dedicated function
  - Interconnecting enclave is responsible for extending IA services such as Identification and Authentication to the interconnection, and for protecting the platform IT from connection risks such as unauthorized access
- Includes the following examples of platform IT interconnections that impose IA considerations:
  - Communications interfaces for data exchanges with enclaves for mission planning or execution
  - Remote administration
  - Remote upgrade or reconfiguration

**Platform IT refers to computer resources, both H/W and S/W, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric.**



# DoD Mission Assurance Categories and Confidentiality Levels

- Information assurance requirements have traditionally been identified through a process of answering four questions: (1) What is the operational value of the information? (2) What is the threat? (3) What statutory and policy requirements must the system satisfy? and (4) What operational, environmental, or technical factors may impact IA solutions?
- DoD Directive 8500.1, *Information Assurance*, establishes how DoD will describe the operational value of information in terms of confidentiality, availability and integrity. It establishes three mission assurance categories that set availability and integrity levels, and three confidentiality levels relative to information classification, sensitivity and need-to-know.
- As early as possible in its life cycle, each DoD information system is assigned a MAC and confidentiality level.



# Mission Assurance Categories

MAC	DEFINITION	Integrity Level	Availability Level
I	Systems that handle information determined to be <b>vital to the operational readiness or mission effectiveness of deployed or contingency forces</b> in terms of both content and timeliness.	HIGH	HIGH
II	Systems that handle <b>information important to the support of deployed or contingency forces.</b>	HIGH	MEDIUM
III	Systems that handle information that is necessary to the conduct of day-to-day business, but <b>does not materially affect support to deployed or contingency forces in the short term.</b>	BASIC	BASIC



# Confidentiality Levels

<b>CONFIDENTIALITY LEVEL</b>	<b>DEFINITION</b>
<b>HIGH</b>	Systems processing classified information.
<b>MEDIUM</b>	Systems processing sensitive information as defined in DoDD 8500.1, to include all unclassified information not explicitly cleared for public release.
<b>BASIC</b>	Systems processing public information as defined in DoDD 8500.1 (i.e., information that has undergone a security review and been cleared for public release).



# DoD IA Controls

- DoD Instruction 8500.2 combines mission assurance categories and confidentiality levels with **consensus or community based best security practices, general threat information, federal and DoD policy requirements**, and enterprise operational and technical considerations (e.g., **interoperability with specific services or supporting IA infrastructures**) in a graded or banded risk model. The model establishes baseline IA requirements for all combinations of mission assurance category and confidentiality level in the form of IA Controls.
- An IA Control is defined as an objective condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control subject area. IA controls are intended to be assignable, actionable, measurable, databaseable, and traceable across an information system's life cycle.



# DoD IA Controls

The DoD IA controls are organized into eight subject areas. The subject areas reflect a defense-in-depth approach, and are drawn from the Information Assurance Technical Framework and supporting IA infrastructures, system life cycle concepts, OMB A-130, and the DoD definition for information assurance.

## SUBJECT AREAS

1. **Security Design & Configuration**
2. **Identification & Authentication**
3. **Enclave & Computing Environment**
4. **Enclave Boundary Defense**
5. **Physical & Environmental**
6. **Personnel**
7. **Continuity**
8. **Vulnerability & Incident Management**



# DoD IA Controls

Together, the MAC and Confidentiality Level identify the baseline set of DoD IA Controls that apply to a DoD information system. The baseline set contains IA Controls from each of the eight subject areas.

Combination No	MAC	Confidentiality	DoDI 8500.2 Enclosure 4 Attachments	IA Control Count
1	MAC I	Classified	1 and 4	110
2	MAC I	Sensitive	1 and 5	104
3	MAC I	Public	1 and 6	79
4	MAC II	Classified	2 and 4	110
5	MAC II	Sensitive	2 and 5	104
6	MAC II	Public	2 and 6	79
7	MAC III	Classified	3 and 4	107
8	MAC III	Sensitive	3 and 5	98
9	MAC III	Public	3 and 6	73



# DoD IA Controls

- DoD IA Controls may be supplemented by Heads of DoD Components and by the system DAA.
- Effectively immediately, DoD IA Controls constitute the baseline requirements for IA certification and accreditation or reaccreditation. The new DoD IA Certification and Accreditation Process (DIACAP) will be organized around IA Controls.
- DoD IA Controls are being integrated into the Joint Quarterly Readiness Reporting System and the Federal Information Systems Management Act (FISMA) reporting requirements.