



Information Assurance (IA): A Different View

Mario Balakgie
Chief Information Assurance Officer
Defense Intelligence Agency

18 April 2000

Form SF298 Citation Data

Report Date <i>("DD MON YYYY")</i> 18042000	Report Type N/A	Dates Covered (from... to) <i>("DD MON YYYY")</i>
Title and Subtitle Information Assurance (IA):A Different View		Contract or Grant Number
		Program Element Number
Authors Balakgie, Mario		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) Defense Intelligence Agency		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Document Classification unclassified		Classification of SF298 unclassified
Classification of Abstract unclassified		Limitation of Abstract unlimited
Number of Pages 22		

REPORT DOCUMENTATION PAGE			<i>Form Approved</i> <i>OMB No. 074-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 4/18/00	3. REPORT TYPE AND DATES COVERED Briefing	
4. TITLE AND SUBTITLE IA: A Different View			5. FUNDING NUMBERS	
6. AUTHOR(S) Mario Balakgie				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) This DIA briefing discusses Information Assurance from a different point of view. It first defines information superiority centered on the network and then looks at the opportunities in this area. It discusses the operations, people, threat, the policy and the technology.				
14. SUBJECT TERMS Information Assurance, Security,			15. NUMBER OF PAGES	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT None	



Information Superiority

- ◆ **Introduces concept of Network Centric Warfare**
- ◆ **Network Power is Combat Power**
- ◆ **Network Defense is Combat Power Protection**
- ◆ **Our information systems strength can become a critical vulnerability**



Opportunities

◆ IT is key to operations

- Warfighter is dependent
- Networks must be reliable



◆ Threats are real

- Explosion in access
- More to protect



◆ People are critical

- Trained and experienced
- Retained and satisfied



◆ Technology must integrate security

- Computing and connectivity
- Software
- User interface and access

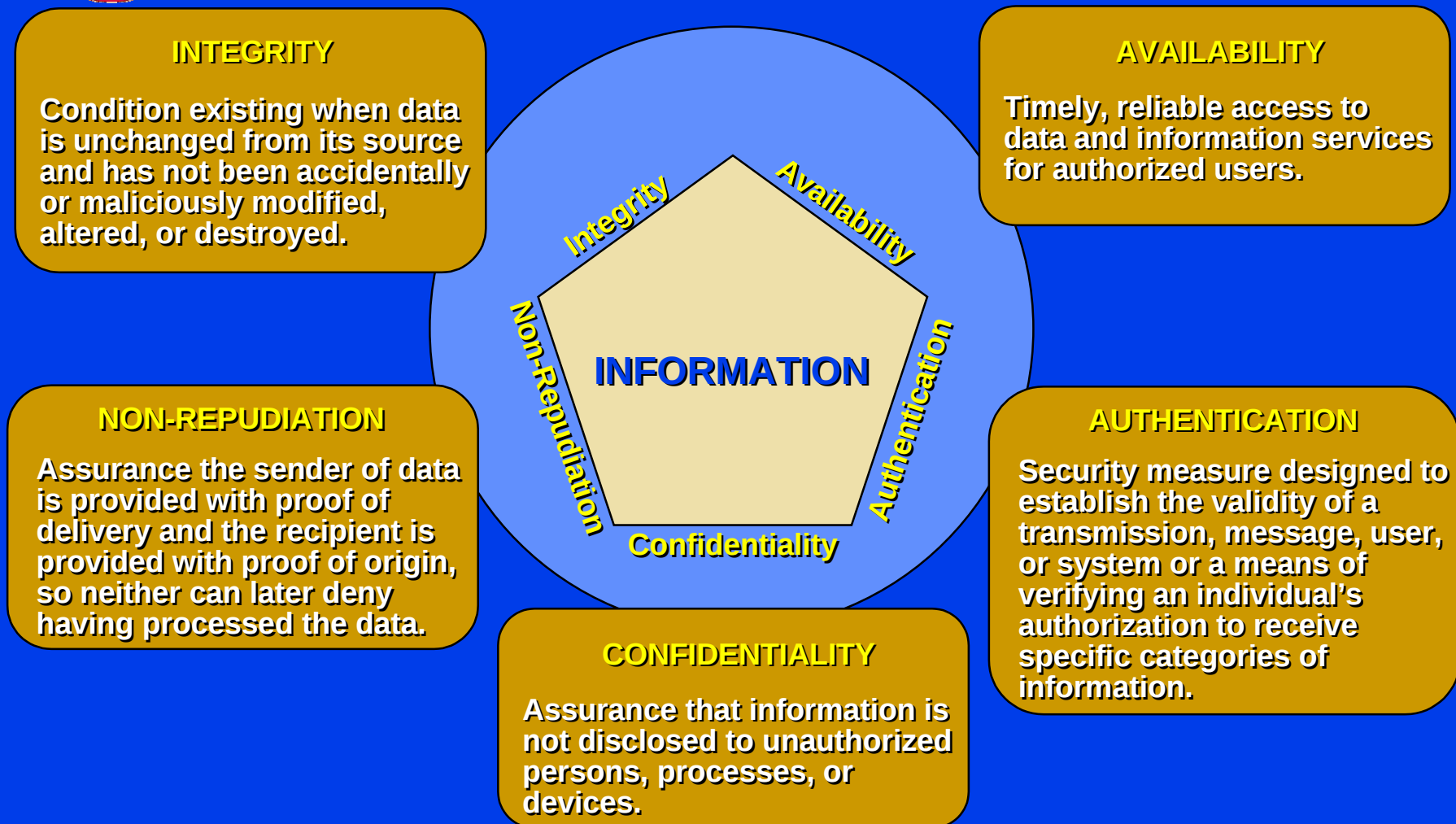
◆ Policy leads integration

- Standards
- Responsibilities
- Direction



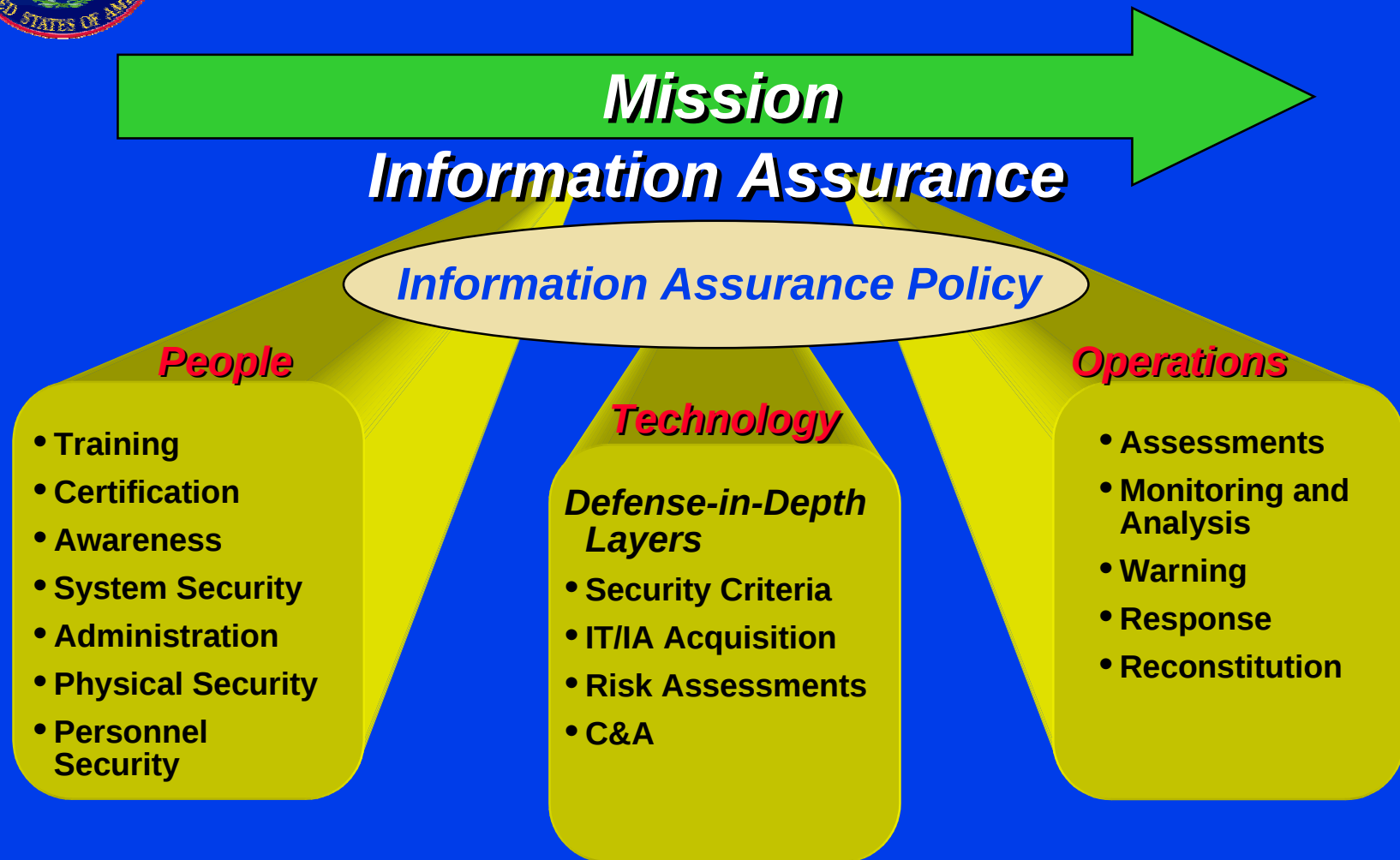


Elements of IA





Multidimensional Approach





Nature of the Business (Problem)

- ◆ **Dynamic environment**
- ◆ **Multiple points of security failures**
- ◆ **Vulnerabilities occur unexpectedly**
- ◆ **Only as strong as the weakest link**
- ◆ **Problem goes beyond the IA professionals**



What Needs to be Done?

- ◆ **Must be enterprise-wide strategy**
- ◆ **Require risk management business practice**
- ◆ **Ensure SCI Infrastructure is reliable and secure**
- ◆ **Priority commitment**
- ◆ **Protect all networks; all classification**
- ◆ **Focus on the human element**
- ◆ **Implement Defense-in-Depth**



How do we get there?



Defense-in-Depth

- ◆ **Protect the network**
- ◆ **Protect the enclave**
- ◆ **Protect the computing environment**
- ◆ **Public key infrastructure**
- ◆ **Detect and respond**

Strategic Partnership



Protect the Network

- ◆ Confidentiality
- ◆ Availability
- ◆ Integrity



JWICS

Network Operations Center

- ◆ Network Management
- ◆ Visibility
- ◆ Encryption (Type 1)
- ◆ Router-to-Router

Switches/Router
Management
and Security



Local Network Operations

Site Infrastructure
(DoDIIS and non-
DoDIIS)

Enterprise Infrastructure
Protection

- Security Services



Protect the Enclave



Router
Filtering

Firewall

Site Infrastructure
(SCI) (DoDIIS and
non-DoDIIS)

Enterprise
Infrastructure
Protection

Non-SCI

Approved
Controlled
Interface
(Guard)

Unclassified

Network Operations Center

- ◆ Intrusion Detection
- ◆ INFOCON Alert
- ◆ Enterprise-wide assessment of controlled interface
- ◆ Re-validate req for controlled interface
- ◆ Reduce numbers
- ◆ Concentrate on approved list



Protecting the Computing Environment

- ◆ Access Management
- ◆ Audits
- ◆ Intrusion detection
- ◆ Virus protection
- ◆ Configuration Management
- ◆ Operation System Security
- ◆ PKI applications
- ◆ Vulnerability assessments



User Workstation

- ◆ Information System Security Management critical to success
- ◆ Chief Information Officer role
- ◆ Protection against the insider
- ◆ Manage and license system administrators



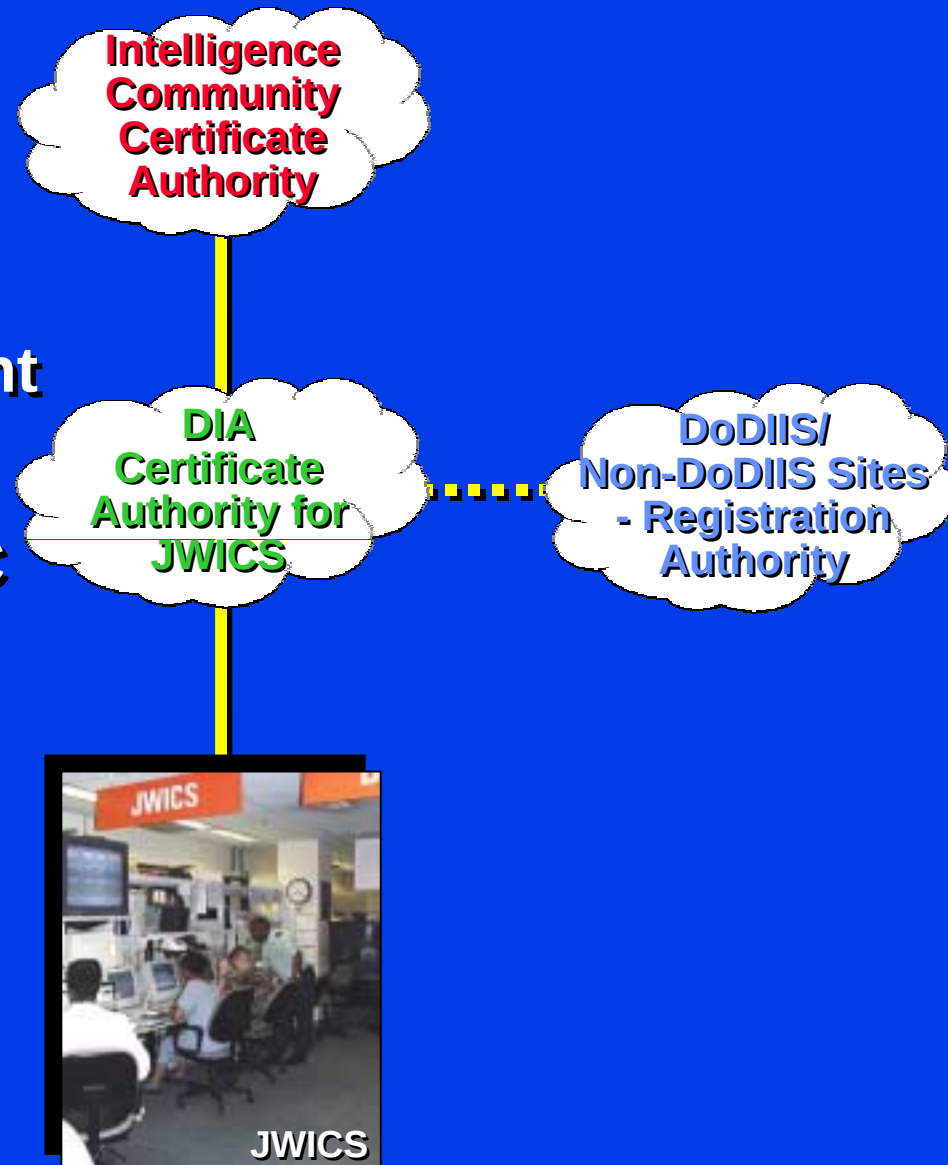
Servers

Web application
Mission application



Public Key Infrastructure

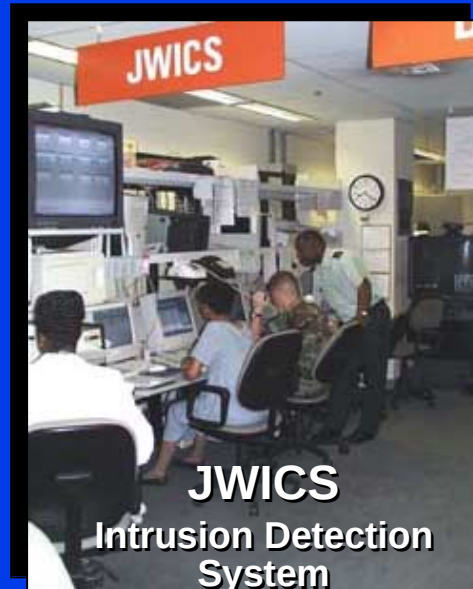
- ◆ Enterprise-wide management
- ◆ Operations emphasis
- ◆ Single approach DoD and IC
- ◆ Design and architecture being evaluated
- ◆ DMB action item





Detect & Respond

- ◆ Monitor
- ◆ Analyze
- ◆ Respond
- ◆ Report



Network Operations Center

- ◆ Monitoring
- ◆ Computer Network Defense (CND)
- ◆ Enterprise-wide management

Site Infrastructure
(DoDIIS and non-DoDIIS)

- ◆ Internal Intrusion Detection System Report (CND)



Initiatives

- ◆ **Development of DODIIS IA Strategy**
 - **Coordinate with DMB**

- ◆ **Modeling an IA business process & risk management practice**
 - **Automated tool**



Conclusion

- ◆ Enterprise wide IA management is essential
- ◆ Apply disciplined business process
- ◆ Risk management practice required
- ◆ New growth area with demanding environment



The Face of IA



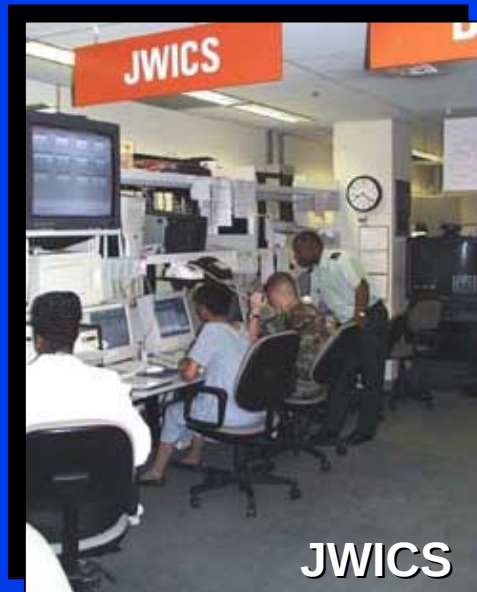
***Any
questions?***



Questions and Comments



Protect the Enclave



JWICS

Network Operations Center

- ◆ Intrusion Detection
- ◆ INFOCON Alert

- ◆ Enterprise-wide assessment of controlled interface
- ◆ Re-validate req for controlled interface
- ◆ Reduce numbers
- ◆ Concentrate on approved list

Router Filtering



Firewalls



Site Infrastructure (SCI) (DoDIIS and non-DoDIIS)

Approved Controlled Interface (Guard)

Non-SCI

Unclassified



Big IA Brother is Watching You!





Mission

- ◆ **The primary function of IA is to advise the decisionmaker of risks by assessing and recommending methods to reduce those risks to the information infrastructure**

Institutionalize Business and Risk Management Processes