Information Assurance (IA): A Different View

Mario Balakgie
Chief Information Assurance Officer
Defense Intelligence Agency

18 April 2000
# Form SF298 Citation Data

<table>
<thead>
<tr>
<th>Report Date</th>
<th>Report Type</th>
<th>Dates Covered (from... to)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(&quot;DD MON YYYY&quot;)</td>
<td>N/A</td>
<td>(&quot;DD MON YYYY&quot;)</td>
</tr>
<tr>
<td>18042000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title and Subtitle</th>
<th>Contract or Grant Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Assurance (IA): A Different View</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authors</th>
<th>Project Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balakgie, Mario</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performing Organization Name(s) and Address(es)</th>
<th>Performing Organization Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense Intelligence Agency</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sponsoring/Monitoring Agency Name(s) and Address(es)</th>
<th>Monitoring Agency Acronym</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distribution/Availability Statement</th>
<th>Monitoring Agency Report Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release, distribution unlimited</td>
<td></td>
</tr>
</tbody>
</table>

| Supplementary Notes | |
|---------------------||

| Abstract | |
|----------||

| Subject Terms | |
|---------------||

<table>
<thead>
<tr>
<th>Document Classification</th>
<th>Classification of SF298</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification of Abstract</th>
<th>Limitation of Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

| Number of Pages | |
|-----------------||
| 22              | |
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.
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

- People are critical
  - Trained and experienced
  - Retained and satisfied

- Policy leads integration
  - Standards
  - Responsibilities
  - Direction

- Threats are real
  - Explosion in access
  - More to protect

- Technology must integrate security
  - Computing and connectivity
  - Software
  - User interface and access
**Elements of IA**

**INTEGRITY**
Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

**NON-REPUDIATION**
Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of origin, so neither can later deny having processed the data.

**CONFIDENTIALITY**
Assurance that information is not disclosed to unauthorized persons, processes, or devices.

**AVAILABILITY**
Timely, reliable access to data and information services for authorized users.

**AUTHENTICATION**
Security measure designed to establish the validity of a transmission, message, user, or system or a means of verifying an individual’s authorization to receive specific categories of information.

* Source DIAP
Multidimensional Approach

Mission

Information Assurance

Information Assurance Policy

People
- Training
- Certification
- Awareness
- System Security
- Administration
- Physical Security
- Personnel Security

Technology
- Defense-in-Depth Layers
  - Security Criteria
  - IT/IA Acquisition
  - Risk Assessments
  - C&A

Operations
- Assessments
- Monitoring and Analysis
- Warning
- Response
- Reconstitution

* Source DIAP
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

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

JWICS
Protect the Enclave

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

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

Enterprise Infrastructure Protection

Non-SCI

Approved Controlled Interface (Guard)

Unclassified
Protecting the Computing Environment

- Access Management
- Audits
- Intrusion detection
- Virus protection

- Configuration Management
- Operation System Security
- PKI applications
- Vulnerability assessments

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

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

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

Approved Controlled Interface (Guard)

Non-SCI

Unclassified
Big IA Brother is Watching You!
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.