DEVELOPING THE INFORMATION WARFARE DEFENSE: A DISA PERSPECTIVE

ROBERT L. AYERS
CHIEF, INFOSEC PROGRAM MANAGEMENT OFFICE

12/04/1995
<table>
<thead>
<tr>
<th><strong>Form SF298 Citation Data</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report Date</strong></td>
</tr>
<tr>
<td>&quot;DD MON YYYY&quot;</td>
</tr>
<tr>
<td><strong>Report Type</strong></td>
</tr>
<tr>
<td>N/A</td>
</tr>
<tr>
<td><strong>Dates Covered (from... to)</strong></td>
</tr>
<tr>
<td>&quot;DD MON YYYY&quot;</td>
</tr>
<tr>
<td><strong>Title and Subtitle</strong></td>
</tr>
<tr>
<td>Developing the Information Warfare Defense: A DISA Perspective</td>
</tr>
<tr>
<td><strong>Contract or Grant Number</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Program Element Number</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Authors</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Performing Organization Name(s) and Address(es)</strong></td>
</tr>
<tr>
<td>DISA</td>
</tr>
<tr>
<td><strong>Sponsoring/Monitoring Agency Name(s) and Address(es)</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Distribution/Availability Statement</strong></td>
</tr>
<tr>
<td>Approved for public release, distribution unlimited</td>
</tr>
<tr>
<td><strong>Supplementary Notes</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Abstract</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Subject Terms</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Document Classification</strong></td>
</tr>
<tr>
<td>unclassified</td>
</tr>
<tr>
<td><strong>Classification of Abstract</strong></td>
</tr>
<tr>
<td>unclassified</td>
</tr>
<tr>
<td><strong>Number of Pages</strong></td>
</tr>
<tr>
<td>71</td>
</tr>
<tr>
<td><strong>1. AGENCY USE ONLY (Leave blank)</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>4. TITLE AND SUBTITLE</strong></th>
<th><strong>5. FUNDING NUMBERS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing the Information Warfare Defense: A DISA Perspective</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>6. AUTHOR(S)</strong></th>
<th><strong>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert L. Ayers</td>
<td>IATAC</td>
</tr>
<tr>
<td></td>
<td>Information Assurance Technology Analysis Center</td>
</tr>
<tr>
<td></td>
<td>3190 Fairview Park Drive</td>
</tr>
<tr>
<td></td>
<td>Falls Church VA 22042</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>8. PERFORMING ORGANIZATION REPORT NUMBER</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>IATAC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense Technical Information Center</td>
</tr>
<tr>
<td>DTIC-IA</td>
</tr>
<tr>
<td>8725 John J. Kingman Rd, Suite 944</td>
</tr>
<tr>
<td>Ft. Belvoir, VA 22060</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>DTIC-IA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>11. SUPPLEMENTARY NOTES</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>12a. DISTRIBUTION / AVAILABILITY STATEMENT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>12b. DISTRIBUTION CODE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>13. ABSTRACT (Maximum 200 Words)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This briefing discusses Defense Information Systems Agency's (DISA) assigned DoD Agent IW-D responsibilities. It provides the current facts about the support that DISA currently provides and the sheer size of that support. The central message is there are current threats to the Defense Information Infrastructure (DII) and that DISA is taking action and measures to defend the DII as part of their mission.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>14. SUBJECT TERMS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>IA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>15. NUMBER OF PAGES</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>16. PRICE CODE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>17. SECURITY CLASSIFICATION OF REPORT</strong></th>
<th><strong>18. SECURITY CLASSIFICATION OF THIS PAGE</strong></th>
<th><strong>19. SECURITY CLASSIFICATION OF ABSTRACT</strong></th>
<th><strong>20. LIMITATION OF ABSTRACT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unclassified</td>
<td>UNCLASSIFIED</td>
<td>UNCLASSIFIED</td>
<td>None</td>
</tr>
</tbody>
</table>
DEVELOPING THE INFORMATION WARFARE DEFENSE: A DISA PERSPECTIVE

DANIEL T. TWOMEY
IW/INFOSEC PMO
INFOSEC PROGRAM MANAGEMENT OFFICE

12/04/1995
Information Warfare

Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our information and information systems...
DISA's IW-D Responsibilities

Director DISA:

will "ensure that DISA Architectures consider EW, ECCM, C3CM"

DODD 3222.4 Electronic Warfare (EW) and Command, Control, Communications Countermeasures, July 31, 1992

is the "Central Manager" of the DII

DMRD 918, September 1992

will "in consultation with the Directors of the DIA and NSA, provide technology and services to ensure the availability, reliability and maintainability, integrity, and security of Defense Information, commensurate with its intended use."

DoDD 8000.1 Defense Information Management Program, October 27, 1992

will "ensure the DII contains adequate protection against attack."

DoDD TS 3600.1, Information Warfare, December 21, 1992

will "assess the vulnerabilities of ... defense information systems" and to "maintain procedures to ensure a capability to respond to identified threats and assessed vulnerabilities"

CJCS MOP 30, Command and Control Warfare, 8 March 1993
DISA's Assigned DoD Agent
IW-D Responsibilities

- Technical Standards
- Training and Courseware
- DoD Computer Emergency Response (Also Army)
- DoD MLS Program
- Goal Security Architecture
- Security Architecture and Engineering Support
- Standardized Certification and Accreditation Policy
- Lead Security Officer Program
- DoD Open IW Contract Vehicles
- Security Product Requirements and Development
- DoD IW-D Management Planning and Management
- DII Protection (IW-D Operations)
DISA FACTS:
MEGACENTER COMPUTERS
Computers in DISA megacenters occupy approximately 14 acres of computer rooms or the space of over 13 football fields.

12/04/1995
DISA FACTS:
MEGACENTER DATA

Data in DISA megacenters could fill over 1,000,000 five drawer file cabinets or over 50,000 average sized personal computers.
DISA FACTS:
MANAGED SATELLITES

DISA managed satellites move more information in a single day than a stack of books 681 miles high.
DISA Digital Networks could circle the globe 400 times or go to the moon and back 21 times
DISA FACTS:
DEFENSE MESSAGING SYSTEM

DISA's DMS serves more users than the entire population of North and South Dakota or Maine or Denver or New Orleans.

12/04/1995
Info Warfare (IW) - Defend

Objective

Assured Information Service
The Defense Information Infrastructure

A seamless web of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing and transport needs of DoD users in peace and in all crises, conflict, humanitarian support, and wartime roles.
The DII
an Infrastructure View

WEAPONS SYSTEMS

SATELLITES

SENSORS

RADIOs

NETWORK SWITCHES

COMPUTERS

VIDEO SYSTEMS

TELEPHONES

MISCELLANEOUS, FAX, MODEMS, PAGERS, ETC.

12/04/1995
Foreign Nations May Conduct Computer Exploitation

Data Corruption

Intelligence Collection

Malicious Software

Denial of Service

Non-Government Threats (Hackers, Terrorists, Organized Crime)

INTERNET

Navy

Air Force

Army

Defense Agencies
DII Threats

- Theft of Service
- Financial Gain
- Jamming
- Malicious Code
- Destruction
- Espionage
- Hackers

12/04/1995
Intruder Technical Knowledge

Technological Knowledge Required

- exploiting known vulnerabilities
- self-replicating code
- password cracking
- password guessing
- disabling audits
- hijacking sessions
- sweepers
- snipers
- diagnostics
- stealth diagnostics
- packet spoofing
- GUI


12/04/1995 053
Reported Security Incidents*

An incident is any event in which a computer system is attacked, intruded into, or threatened with an attack or intrusion.

- 3 1/2 Years of Data
- Doubling Each Year
- Only 1 in 500 Incidents Reported (Estimated)


53 115 255 558 1,222 2,676 5,860 12,633
Approach To The Threat

Yesterday

Risk Avoidance

- Tempest Program
- Physical Isolation
- Certified Products

- Know your vulnerabilities and operate no system with vulnerabilities

Change Dynamics

- Shrinking budget
- Worldwide pursuit for universal connectivity
- Consolidating of DOD's information infrastructure

- Increased reliance on Commercial Products
- Increased reliance on Commercial Service Providers

Risk Management

- Absolute protection is technologically impossible
- Financially impossible to buy absolute protection

- Know your vulnerabilities, operate with them, but manage them

12/04/1995
Information Warfare

Defending The DII

The New Battleground
...AS CENTRAL MANAGER FOR THE DII,
SHALL ENSURE THE DII CONTAINS
ADEQUATE PROTECTION AGAINST ATTACK.

DOD D 3600.1
Cyberspace, a virtual 5th dimension characterized by:

- no geographic, national, or temporal boundaries
- no ownership, laws, or identity cards

The electronic environment formed by the aggregate of global computing and telecommunications resources.
Information Warfare
A New Reality

- Defense information is a target.
  The DII will be the battlefield
  - The world knows we are dependent on information for our style of war
  - Adversaries already have attack capabilities
    - Open literature has examples
    - High school students have succeeded
  - Low cost/high payoff
  - Strategic advantage for low tech armies
DISA INFOSEC
FUNCTIONAL RESPONSIBILITIES

D1
D2
D3
D4
D5
D6
D7
D8

DISA INFOSEC training programs

PMOs:
DII
EC/EDI
GCCS
DMS
DISN

DISA INFOSEC/IW-D program management
Policy
Plans
Resources' Execution
Coordination
GCC/RCC security management operations
ASSIST/VAAP

NCS
NCC

DIRECTOR

CIO

DISA INFOSEC policy
Accreditation of all DISA systems and networks

WESTHEM

RCC operations
DMC operations

CISS

Assessments
Training
Security and Certification

JITC

Security product integration testing

JIEO

Security architecture and engineering
Security product integration
INFOSEC standards MLS

IW-D modeling and simulation
IW-D impact assessments
Security for the DII provided thru a BALANCE of:

PROTECTION: PROTECT critical DII networks, systems and facilities

DETECTION: DETECT attacks upon the DII quickly enough to enable operational reactions

REACTION: Operationally REACT to attacks to either defeat them or maintain service
Red Team Assessment of DoD Security Mechanisms

- Only hacker tools from internet
- Only known vulnerabilities
- Only vulnerabilities covered by prior alerts

12,000 ATTACKS
1,440 BLOCKED (12%)
422 DETECTED (4%)

10,560 SUCCEED
10,138 UNDETECTED

21 REPORTED (5%)
401 NOT REPORTED
10,539 SUCCESSFUL ATTACKS (87.8%)
Historical Roles

Protect
INFOSEC
Certification
Encryption
Passwords
System Isolation

Detect

React
Operations
Fault Isolation
Repair
Performance Balancing
Backup and Recovery
IW-D is a Unifying Mission

Protect    Detect    React
Absolute protection of the entire Defense Information Infrastructure (DII) is neither technically nor financially achievable. Some number of attacks upon the DII will succeed.
PROTECTION Program

Secure critical backbone communications network (DISN) and connection to it

Secure critical military applications:
  Global Command and Control System
  Defense Messaging System
  Business processes (finance, medical, logistics, personnel)

Secure critical processing centers (Defense Megacenters)

Train and equip system administrators for secure operations
DETECTION Program

Continually measure DII vulnerabilities to attack

Develop and implement attack detection technologies

Train and equip security personnel for attack detection
REATION Program

Upgrade DII Global and Regional Control Center System by:

- Adding attack recognition function
- Adding automated infrastructure reaction management capability

Train, equip, and exercise Global and Regional Control Center personnel in defensive information warfare
Secure the Network
World Wide DISN

Defense MegaCenter

Navy Base

AF Base

Army Post

12/04/1995
Secure the Network Infrastructure/Connectivity

Examples

- CONUS/DISN Backbone
- OCONUS Links
- NIPRNET
- SIPRNET
- JWICS Infrastructure
Secure the Applications
Global Command and Control
Secure the Applications
Business Applications & Users

Medical  Personnel  Finance  Logistics
Secure the Applications

GCCS Examples

<table>
<thead>
<tr>
<th>Task Number 4.1</th>
<th>FY96</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procure and Install Multi- Level Security (MLS) Workstations, Trusted Operating Systems and Trusted Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procure and Install Imagery Guard and GCCS/GCCS-T Guard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procure and Install GCCS Intelligence Workstation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port GCCS MLS Software to HP Workstations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O &amp; M for Fielded Systems and Upgrading to New Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Secure the Applications

DMS

Examples

- APIs for Business Systems
- DMS

<table>
<thead>
<tr>
<th>Task Number 4.3</th>
<th>FY96</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMS Implementation (Sensitive but Unclassified)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMS Implementation (Unclassified to Secret)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMS (Interim Top Secret/SCI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Autodin Phase Out</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Multi-Level Secure Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*The DMS Planning depicted above is based on the DMS Migration Strategy as of 18 October 1993 and is under control of the DMS PMO. It is provided as a part of the INFOSEC Plan for information purposes. The Joint Staff approves/disapproves shutdowns of individual AUTODIN Switching Centers (ASCs) on a yearly basis.*
Secure the Defense Megacenters
Secure the Defense Megacenters

DMCs Examples

• Integrate MISSI Technologies
• Standardize Environment
• Certification
• Vulnerabilities
• Security Deficiencies

<table>
<thead>
<tr>
<th>T&amp;k Number 3: 1</th>
<th>FY96</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMC - Columbus EOP</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td></td>
</tr>
<tr>
<td>MVS Systems</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td></td>
</tr>
<tr>
<td>Unisys Systems</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td></td>
</tr>
<tr>
<td>UNIX systems</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td></td>
</tr>
<tr>
<td>Other Systems</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td></td>
</tr>
<tr>
<td>Maintenance</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
</tbody>
</table>
Operate and Manage a Secure DLL

Train Personnel
Certification/Accreditation
Measure Vulnerability
Operate and Manage a Secure DII

Examples

- Certification & Accreditation
- Training
- Red Team
- Security & Ops.
- Mgmt. Integ.

<table>
<thead>
<tr>
<th>Task Number 53.2</th>
<th>FY96</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global C2 System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defense Megacenters Certification/Recertification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DISA-EUR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DISA-PAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIPRNET</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIPRNET</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DISANet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other DISA Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DoD Certification Support (e.g., TACCIMS, EKMS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12/04/1995
Global Control Center
Regional Control Center

Concept
Goal of Global/Regional Control Centers

Significant improvement in military readiness and war fighting capability by:

- Ensuring availability of information services by preventing or operationally reacting to common information system attacks
- Ensuring the confidentiality and integrity of all DoD communications and businesses
Strategic Objectives

Assured Information Service to CINCs

Battlespace Management (DISA is Cyberspace Warfighter)

Integration into Worldwide Warning Indicator Monitoring System (DIA Support)

Integration into National Military Command and Control System

Tie to National SIGINT Operations Center (NSA Support)
Center Connections

DII

Worldwide Warning Indicator Monitoring System (DIA Support)

National Military Command and Control System

DISA

National SIGINT Operations Center (NSA Support)
Proactive detection and reaction
 Hierarchical Relations
 Routine vs 'Crisis Operational Modes
 Nominal Control Center Model
Global/Regional Control Center
A Functional View

Security/Operations

- NMCCSC Officer
- DISN Officer
- PSN(NCS) Officer

Operations/Security

- Duty Officer
- DIA Warn Officer
- PC Officer
- Satellite Officer

12/04/1995
Global/Regional Control Center
A Functioning View

DISN
Ops Sec
Sec Ops

LAN
Ops Sec
Sec Ops

PCs
Ops Sec
Sec Ops

DMC
Ops Sec
Sec Ops

PSN(NCS)
Sec Ops
Ops Sec

Spectrum

Video

Satellites
Sec Ops
Ops Sec
Sec Ops
Sec Ops

Global/Regional Control Center
A Functioning View
Hierarchical Relations

- Audit data collection Points

Local Environment

- GCC
- PSN
- RCC
- RCC
- RCC
- RCC
- BLCC
- DMC
- BLCC
Operating Modes
Routine Operations

Global Control Center

RCC - RCC - RCC - RCC

Red = Detection
Blue = Reaction
Green = Reporting

12/04/1995
Operating Modes
Crisis Operations

Global Control Center

RCC
RCC
RCC
RCC

Red = Detection
Blue = Reaction
Green = Reporting

12/04/1995
GCC/RCC Functions

Vulnerability Detection (Continual VAAP)
Attack Recognition (AMIDS)
Prioritized Responses (AIMS)
Customer Support (BBSs/Alerts/Tools)
CINC Support Team
IW-D Battlespace
Wargames and Exercises
Incident Response (DoD, National, International)

12/04/1995
GCC/RCC Requirements

Audit Monitoring/Intrusion Detection (AMIDS)
Malicious Code Detection Eradication (h&DES),
Automated Infrastructure Management (AIMS)
Vulnerability Analysis (VAAP)
Personnel, Training, and Facilities
Wargames and Exercises
Reserve Components
Audit/Monitoring
Intrusion Detection System

Mainframe

PC

Network Nodes

Servers

Audit data

Data Reduction Threshold

Security Officer

Security Officer

12/04/1995
Audit Monitoring/
Intrusion Detection System

Detect unauthorized activity as it occurs

Examples

- Intrusions
- Password Attacks
- Increased Privilege
- Disabling of Audits
- Denial of Service

<table>
<thead>
<tr>
<th>Task Number 5.5.1</th>
<th>FY96</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify, Evaluate, and Select COTS/GOTS AMIDS</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Acquire and Field Systems Hardware and Software</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Integrate and Standardize AMIDS Product Across Heterogeneous Operating Systems</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Expand Capabilities of Selected Products</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Maintain AMIDS</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
</tbody>
</table>

* FY96 activities conducted with Government manpower and resources

12/04/1995
Malicious Code Detection/Eradiation System

Today

Virus introduced into computer

Planned

Detects malicious code before introduction into DII computer
Malicious Code Detection Eradication

Normal Operations

Local Environment

Central System

Push Updates

Pull New Systems/Updates

12/04/1995
Malicious Code Detection Eradication

Contingency Operations

Local Environment

Central System

Push Down Full File Replacement
Malicious Code Detection
Eradication System

Detect Irregular Code

Examples

- Viruses
- Trojan Horses
- Time Bombs
- Spoofing Tools
- Sniffers
**Example Responses**

- Alternate Network Routing
- Prioritized Network Service Levels
- Move Service From Digital Networks To Satellite Systems
- Frequency Re-allocation
- Communications Isolation
- Response Team Dispatch
- Fall Back Processing
- NSEP Activation
- "Patch" Development and Deployment
Automated Infrastructure Management

Manage and Control the DII Under Attack

Examples

- Terrestrial/Satellite
- Isolation
- Restoral
- Alternate Routing
- Fallback Processing

<table>
<thead>
<tr>
<th>Task Number 5.5.4</th>
<th>FY96</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigate Existing Capabilities</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select, Modify, and Integrate AIMS</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field AIMS in GCC/RCCs</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain and Enhance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*FY96 activities conducted with Government manpower and resources
Vulnerability Analysis and Assessment Program

Detect Potential Problems in Systems

Targets

- Assessments
- Components
- Procedures
- Facilities
- Personnel

<table>
<thead>
<tr>
<th>Task Number 5.4.2</th>
<th>FY96</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct UNIX Systems Vulnerability Assessments</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Conduct Mainframe Computing Systems Vulnerability Assessments</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Conduct Networking Vulnerability Assessments</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Conduct Telephony Vulnerability Assessments</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>Conduct Vulnerability Assessments on Other Systems (e.g., PCs, Environmental Controls)</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
</tbody>
</table>
Personnel and Training

Prepare People to Support GCC/RCC

Examples

- Info-warrior
- Retrain
- SCI Cleared
- 200 Security Personnel
- Reserve Components Utilization Plan

<table>
<thead>
<tr>
<th>Task Number</th>
<th>FY96</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.5B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrain RCC Specialists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain the Facilities and Technical Proficiency Training Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Facilities

Prepare People & Facilities to Support GCC/RCC

Examples

- SCIF is Required
- Backup Site
- Power (UPS)
- Equipment (AIS/Housekeeping)
- Communications (New/Redundant)
Wargames and Exercises

Practice and Test Plans

Examples

- Red Team
- Prototype
- Implement
- Exercise

<table>
<thead>
<tr>
<th>Task Number 1.5</th>
<th>FY96</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Red Team</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational Concepts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop Wargame and Exercise Concepts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop and Test Prototype Wargames and Exercises</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop and Implement Wargames and Exercises</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Include Exercises in Joint Exercises</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reserve Components

Augment with Experts

Examples

- Peacetime Tests
- Contingency
- Expertise
- Practice

<table>
<thead>
<tr>
<th>Task Number 1.6</th>
<th>FY96*</th>
<th>FY97</th>
<th>FY98</th>
<th>FY99</th>
<th>FY00</th>
<th>FY01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop CONOPS and Realign Reserve Utilization in DISA for IW-D/INFOSEC Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide Increased IW-D/INFOSEC Support to GCC/RCC/DMCs and MSTs in Peacetime, Exercise and Contingency Crisis Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*FY96 activities conducted with Government manpower and resources
Examples

- Architecture and Engineering
- Standards
- Testing
- Tech. Insert.

Modeling & Sim.
INVESTMENT Program

Research and development to:

Maintain technological currency of existing security products

Develop new security products for digital networks:

- Replace analog secure (STE) with digital secure telephone (STU-III)
- Secure digital cellular (wireless) telephone capability
- Secure high-capacity, digital broadcast capability for tactical forces
Information Warfare
Response To A New Reality

- Defense planning must reflect anticipated realities
  - Battle damage assumed, operation under stress
  - Response procedures and recovery capacity built in

- Priorities must be properly addressed:
  - Infrastructure
  - Operations

- Criticality of information must be understood
  - Operational need/impact of loss - time critical

- We must train for defensive information warfare
  - Train information warriors
  - Hold wargames, readiness drills and exercises