IA-00016

Managing Information Security Problems

Clarence Hoop
Chief, Plans, Policy & Integration Division
DISA CISS
Phone: (703) 681-7988
hoopc@ncr.disa.mil

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01011996	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Managing Information Security Problems	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) DISA	**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 34	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	1/1/96	Briefing

4. TITLE AND SUBTITLE
Managing Information Security Problems

5. FUNDING NUMBERS

6. AUTHOR(S)
Clarence Hoop

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 DISA Briefing discusses the topic of Managing Information Security Problems. The areas the briefing covers are: The operational environment; what are some of the problems encountered; what is happening in the community today and what are the community plans for the future. It addresses the issues of insider threat, external threat, how to cope with the threats, use of firewalls and the Defense in Depth strategy.

14. SUBJECT TERMS
IA

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Presentation Outline

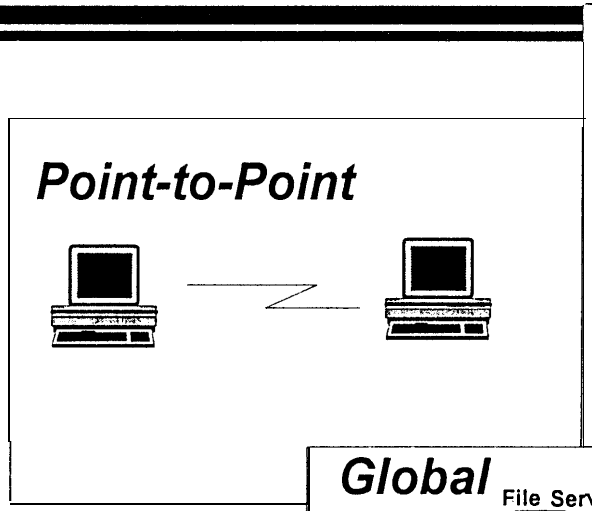
What is the Operational Environment?

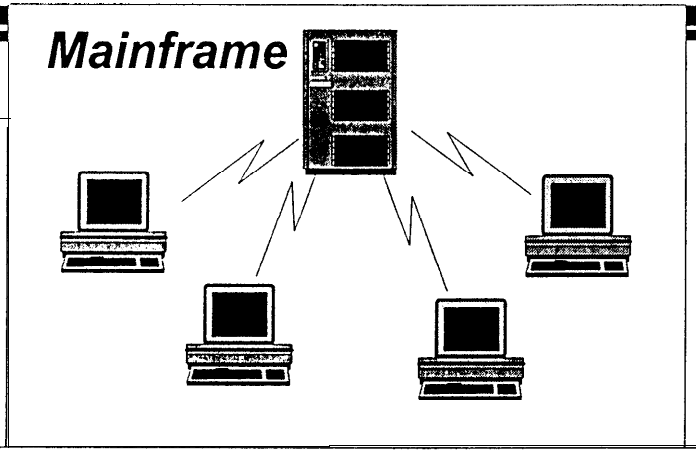
What are some of the problems encountered?

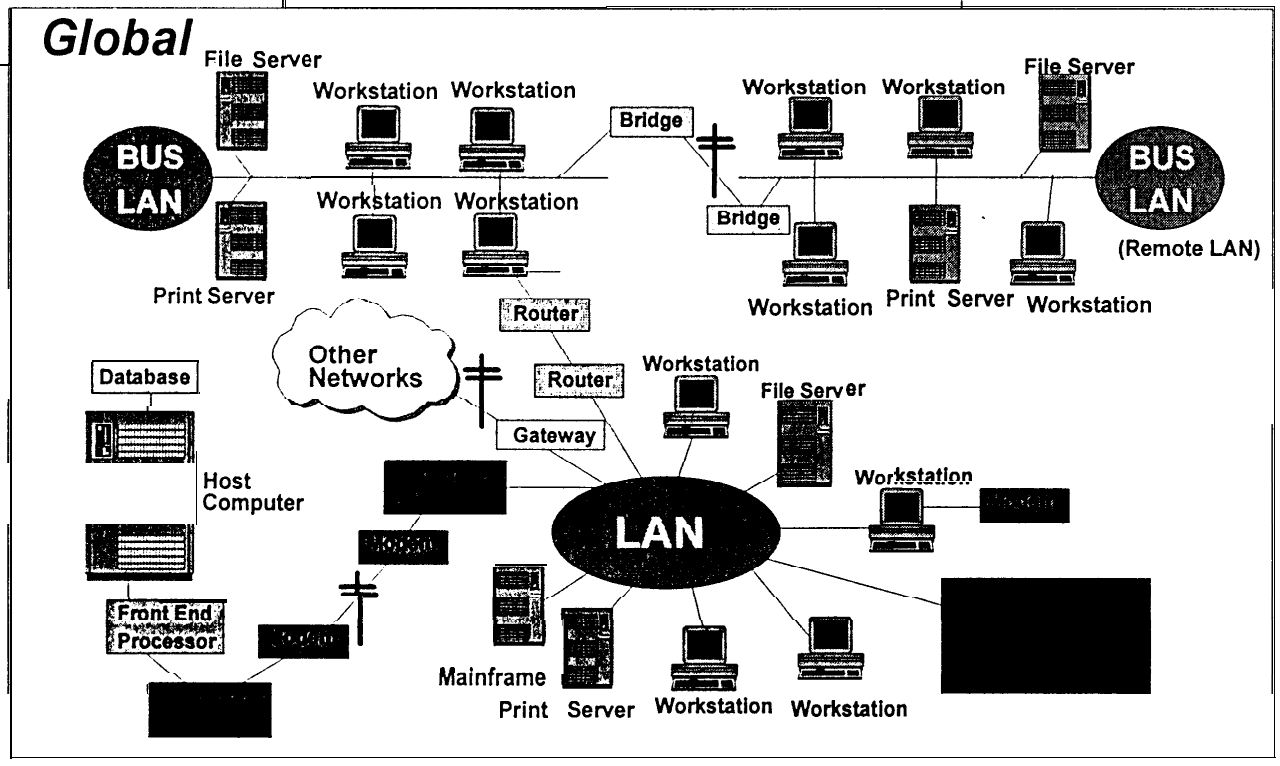
What are we doing today?

What do we plan for tomorrow?

Technology Revolution



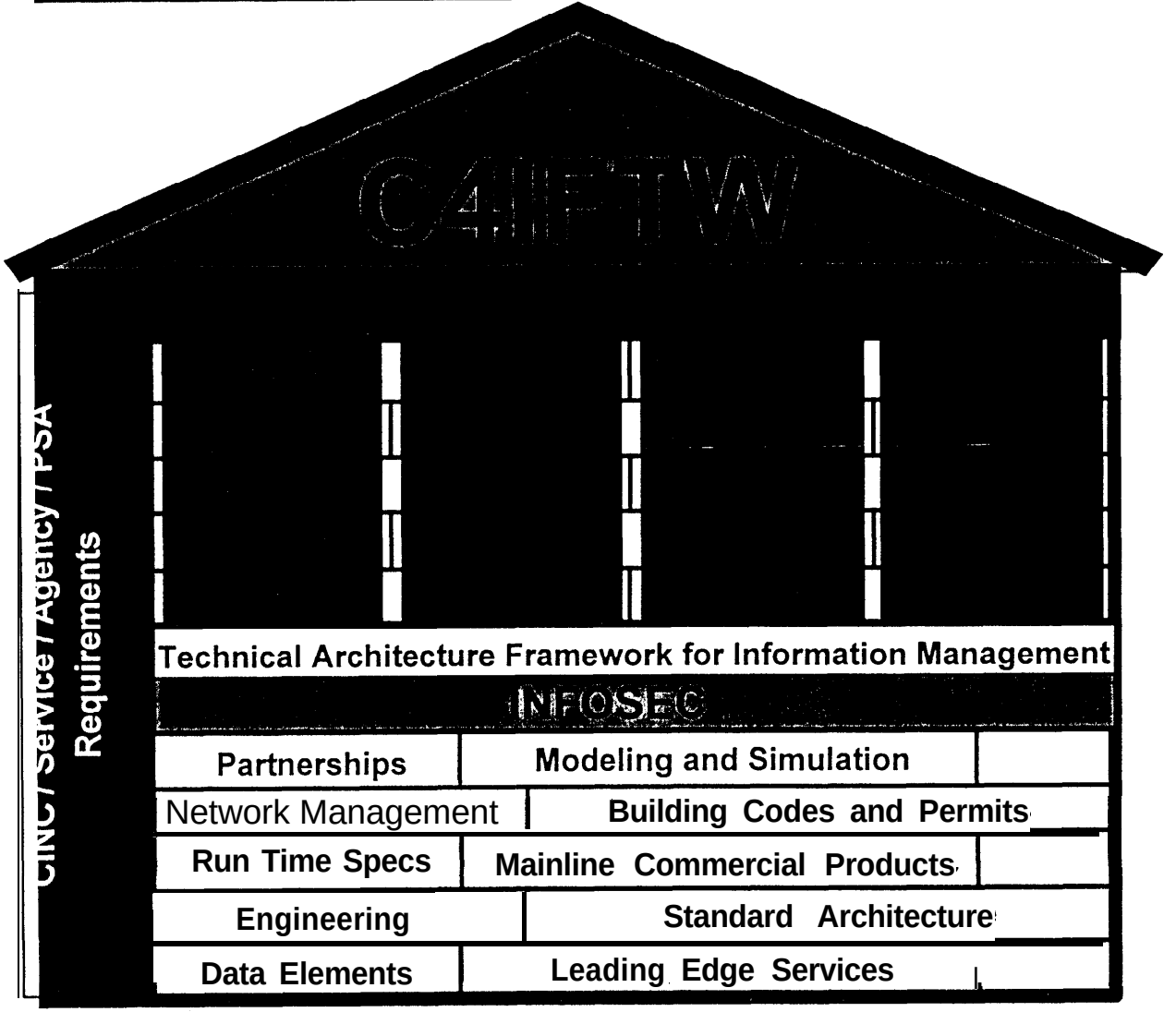


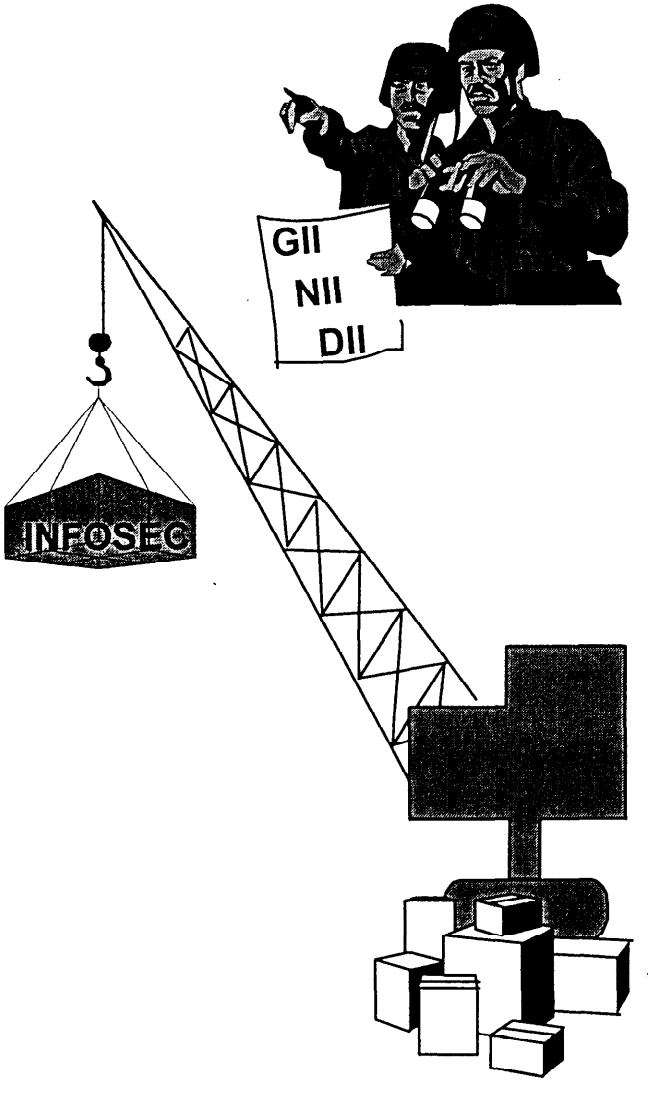


DISN

- ✓ Transmission
- ✓ Command & Control
- ✓ Messaging
- ✓ Combat Support

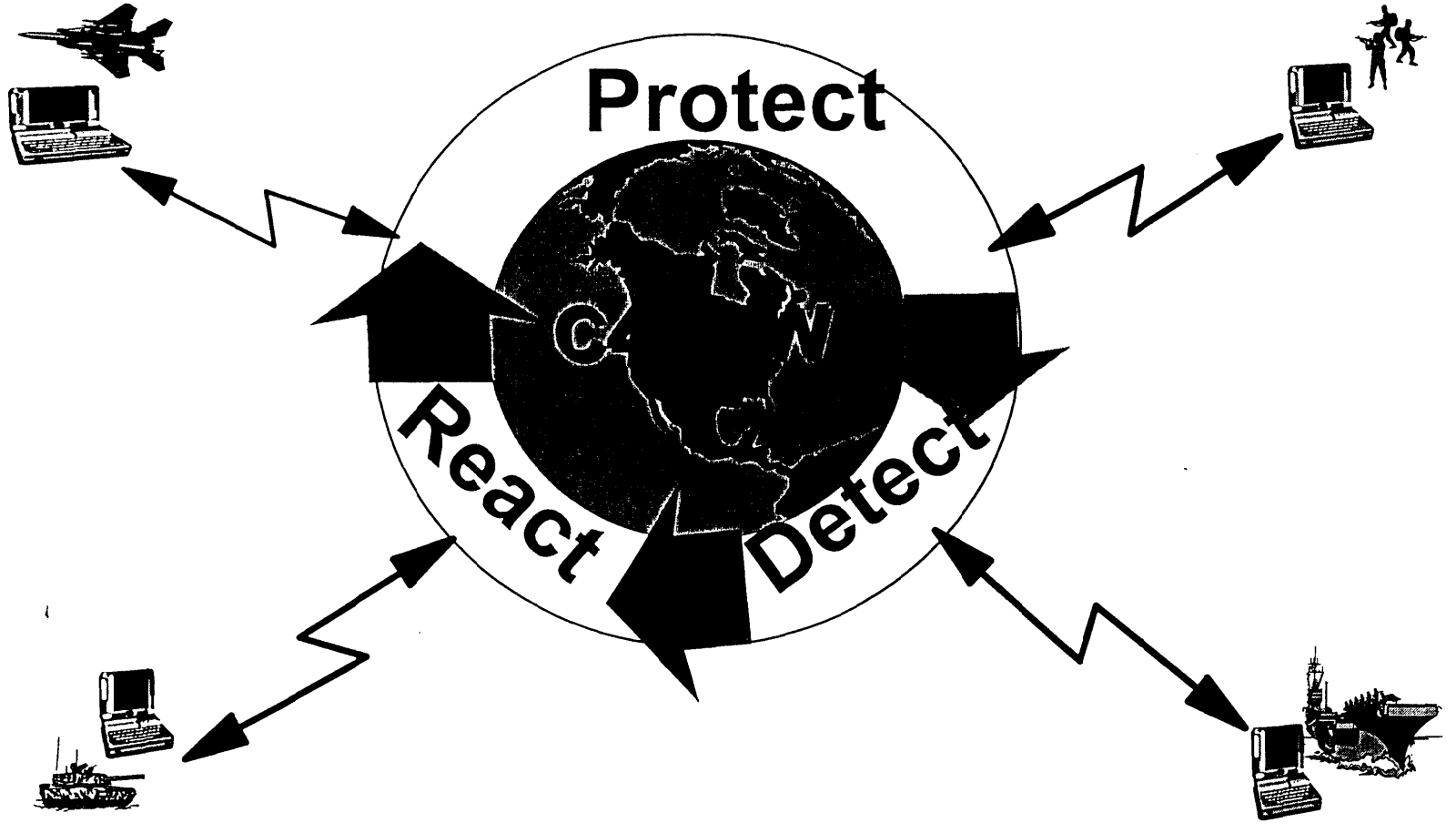
C4I for the Warrior





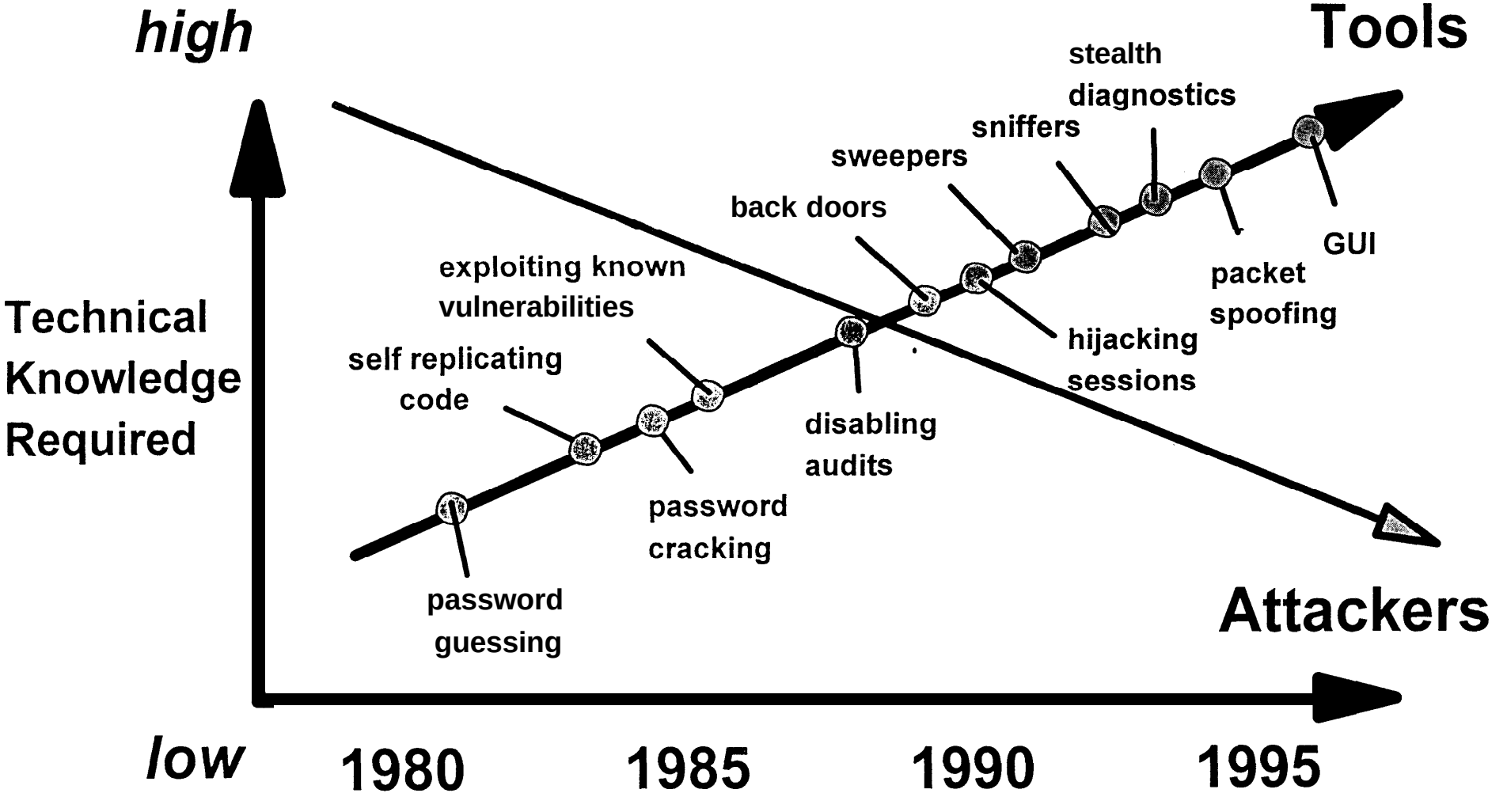
DISA: ARCHITECT OF THE FUTURE

DISA INFOSEC STRATEGY:
Supporting the DISN Mission

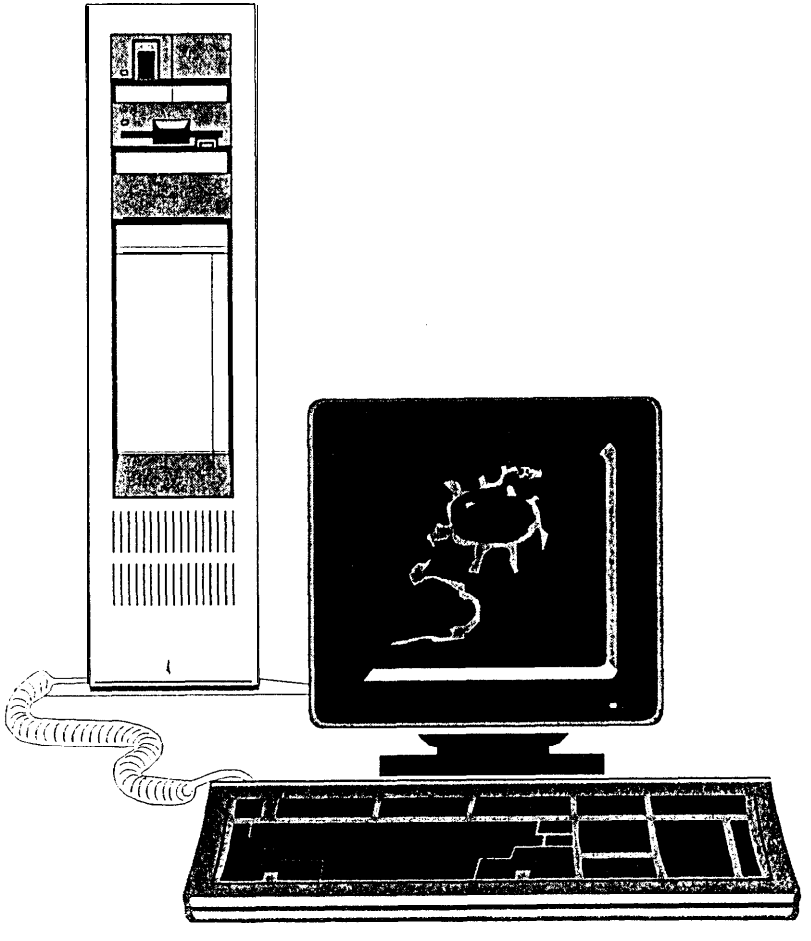


Defend the DII: Anywhere, Anytime, Any Mission

Intruder Technical Knowledge

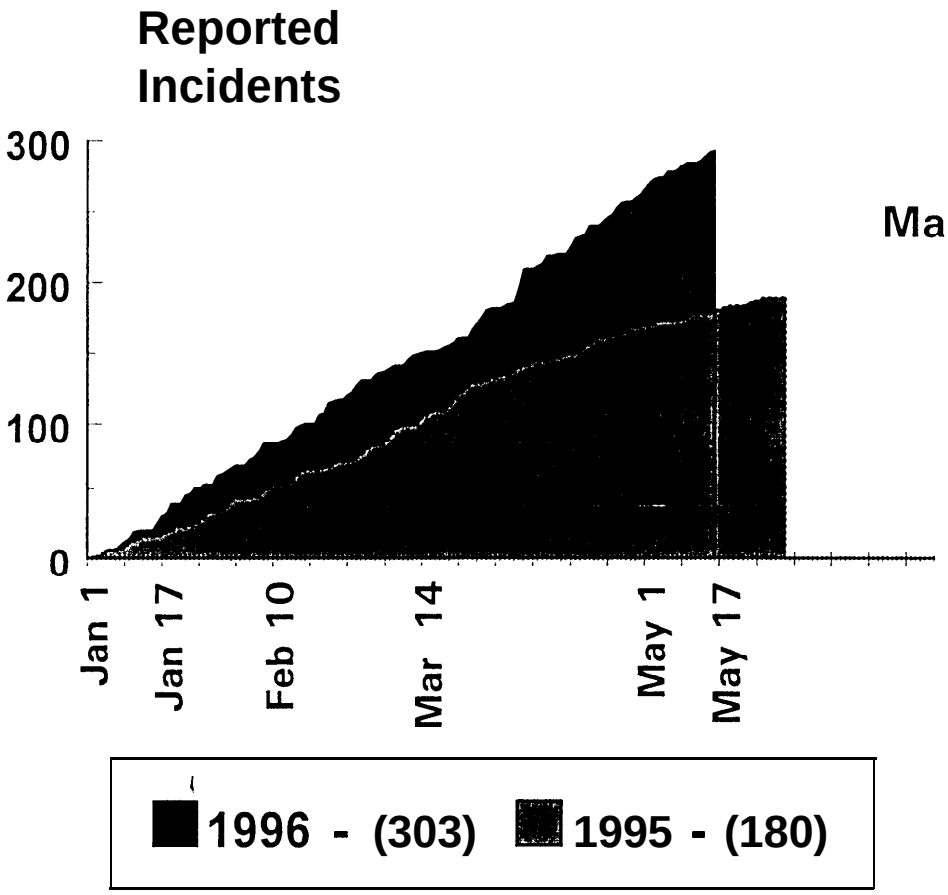


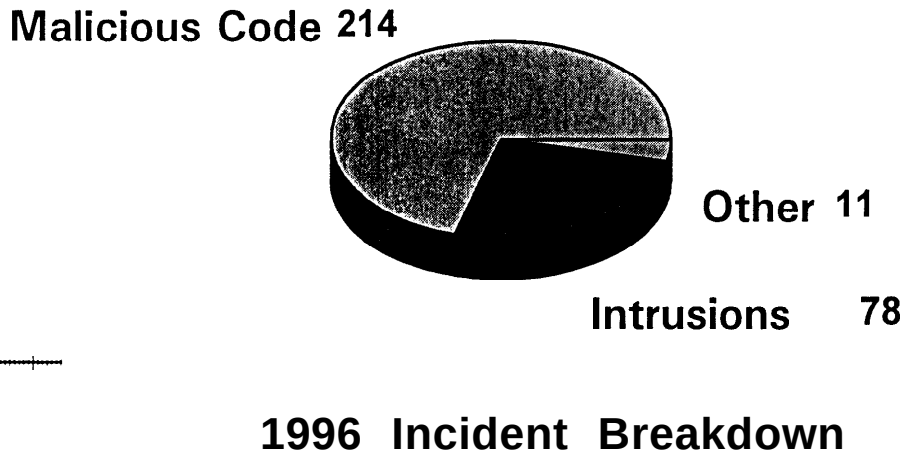
Intruders Have Been Observed



- Destroying data
- Destroying software
- Modifying Data
- Modifying software
- Stealing data
- Stealing software
- Shutting down hosts/networks
- Using **DoD** systems as launch points

Incidents Reported to DISA/ASSIST





As of 2400 hrs 23 May 96

What do we see at ASSIST?

Tools & Techniques

- Telnet/ftp
- Password Files/tftp/Crack
- Sendmail/smtp
- Sweepers
- finger
- Sniffer
- r* commands
- IP spoofing
- Rootkit

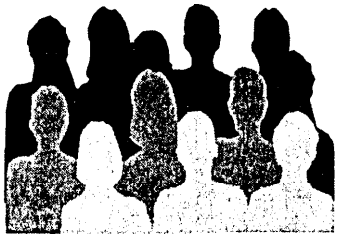
What do we see at ASSIST?

Virus Contenders

- Word Marco Virus
- Monkey
- Form
- BUPT
- AntiExe
- Jack the Ripper

Where do they get those toys?

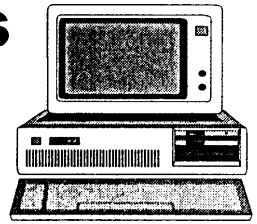
Newsgroups



FTP Sites

WEB Pages

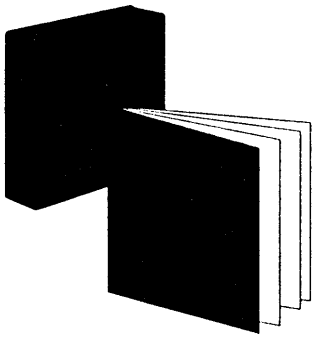
BBSs



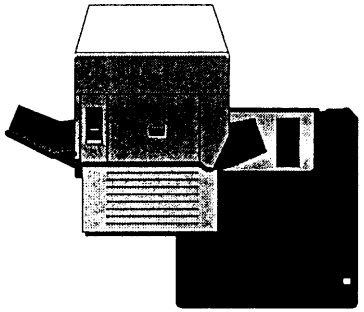
Books

Magazines

Ezines



Trade



An Example of DoD Functions Affected

Composite Material Research

Structural Research on Ships/Planes

Personnel Management Services

Ballistic Weapons Research

R&D on Health Sciences

R&D on Ocean Sciences

Inventory and Property Accounting

Organizational Service Training

Payroll and Business Support

Finite Element Analysis of Submarine Structures

Mathematical Simulations

Supply and Maintenance Support System

Master Clock for 1/4 of the WORLD

Command Tasker System

Mail Hub for Post-wide Electronic Mail

Finance Databases

Procurement

Scientific Modeling for Battlefield Environment

C3 Development

Ocean Surveillance

Military Health Systems

High Performance Computing Systems

Supercomputer Research Network

Artificial Intelligence Research

Knowledge Based Simulation

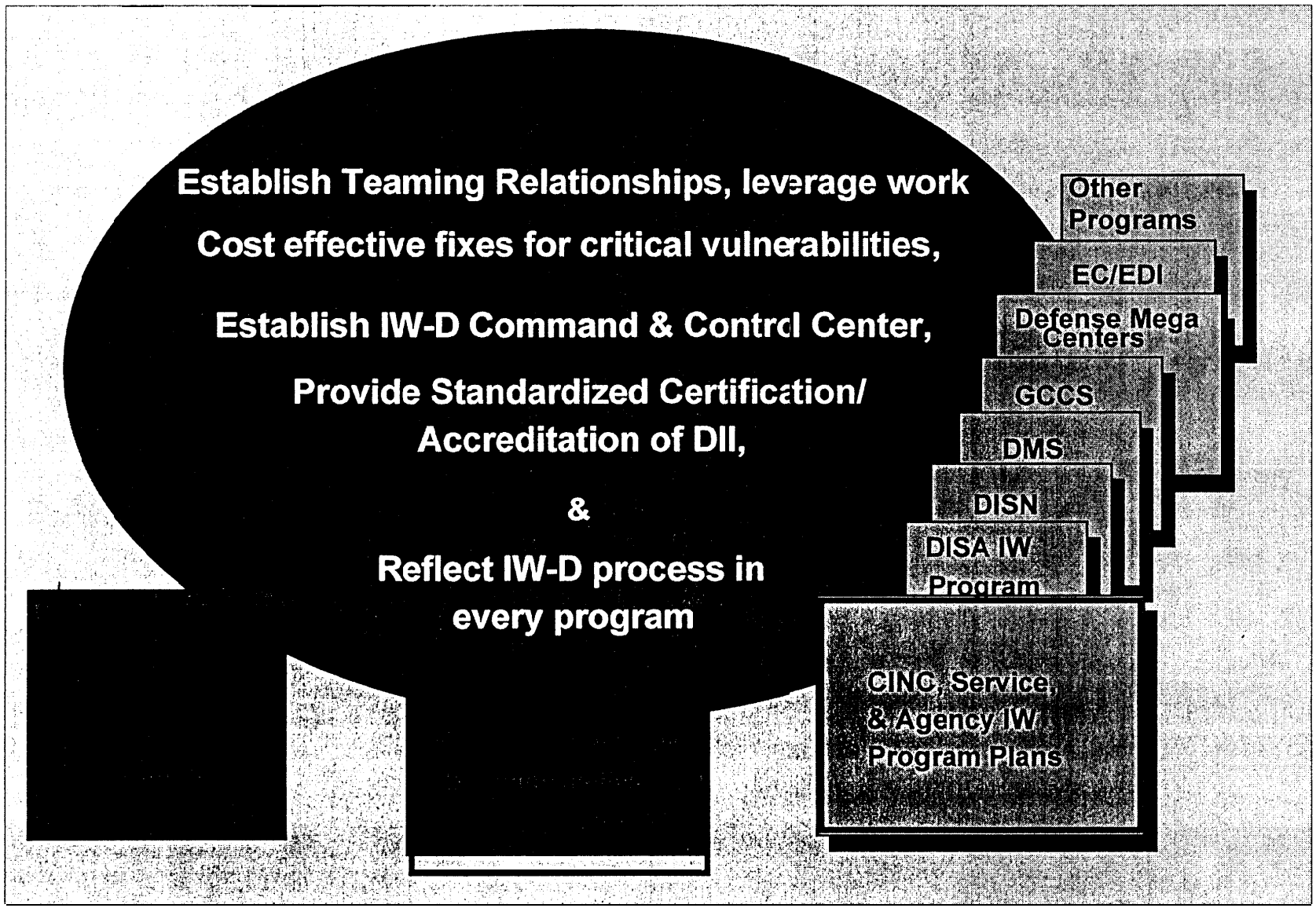
Applied Research in Photonic Technology

Force Level Execution

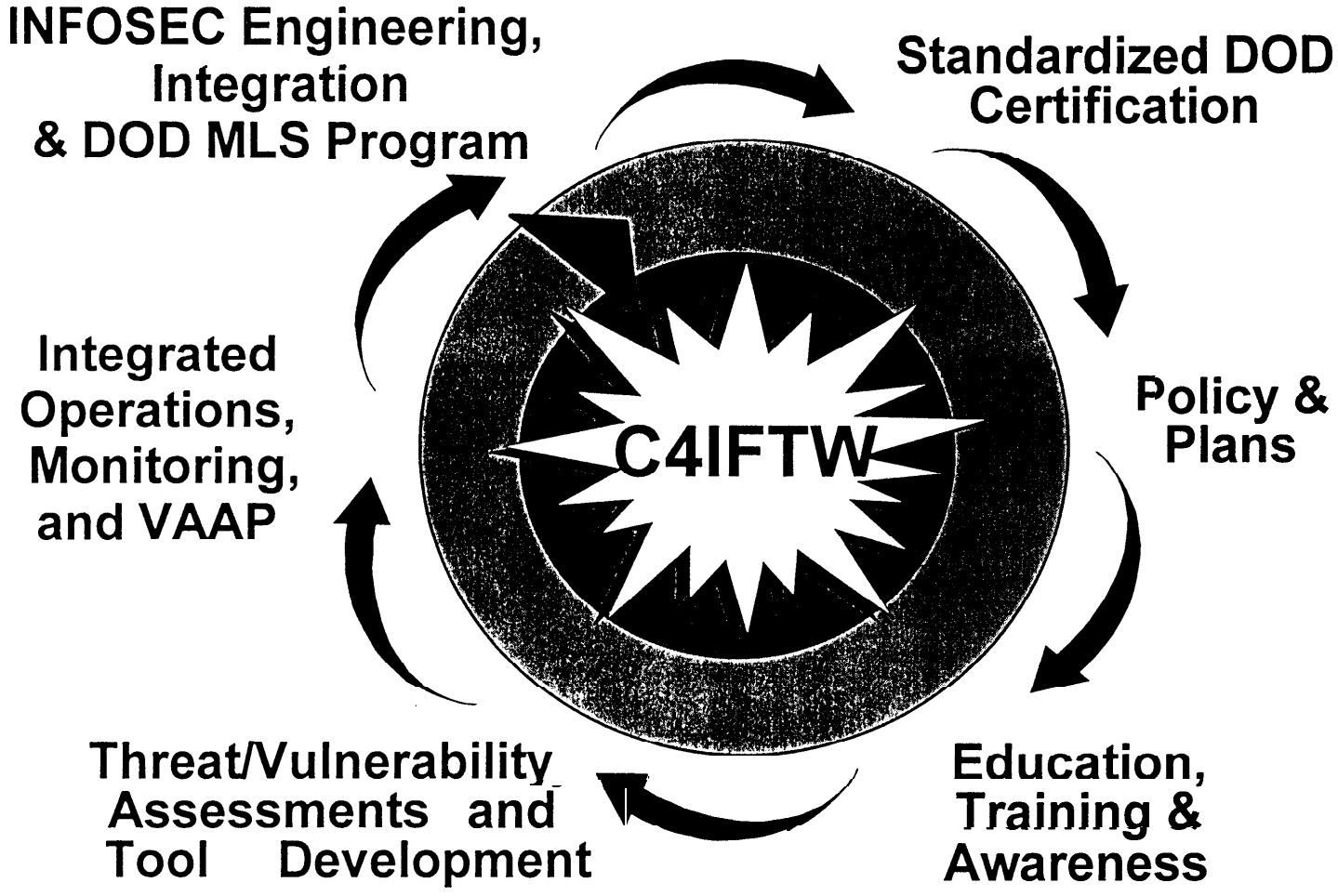
Battle Management Decision Aids (Presentation)

INFOSEC Functions

VISION & STRATEGY FOR DEFENSIV≤ INFORMATION WARFAR≤



DISA's Multi-Disciplined Security Process



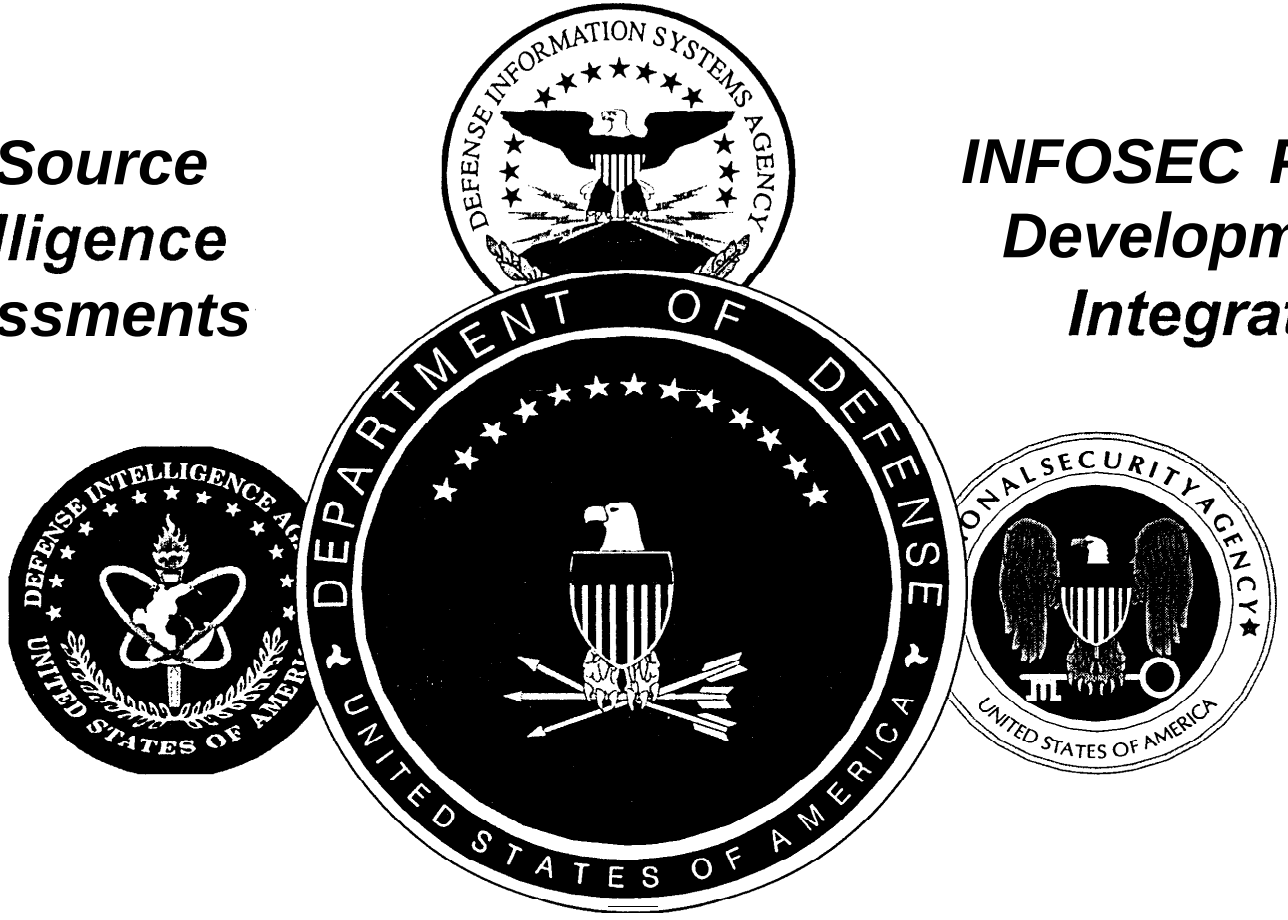
INFOSEC Technical Services Contract

Collaborative Work Environment

Defend the DII

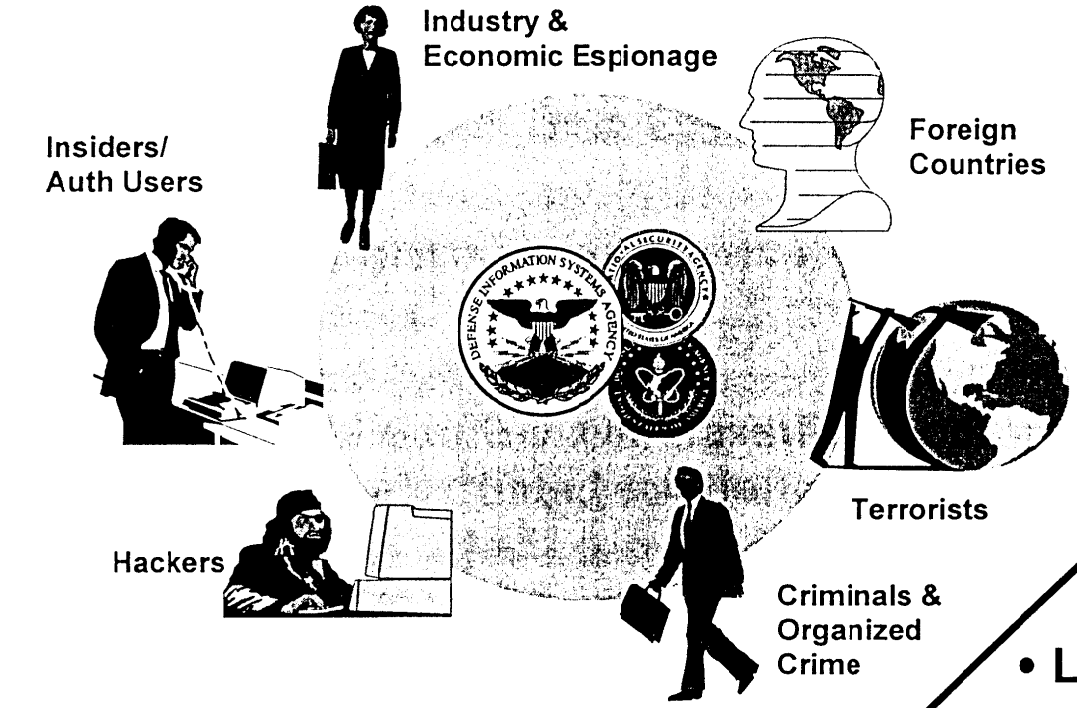
All Source Intelligence Assessments

INFOSEC Product Development & Integration



FOCUS: Get INFOSEC Products to the Warfighter!

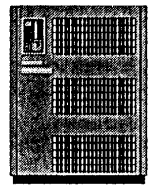
Threat & Vulnerability



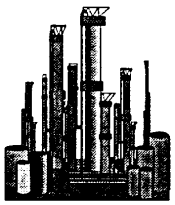
Threat Assessments

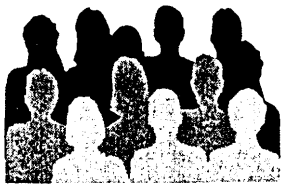
Vulnerability Assessments

- Technical Vulnerabilities
  - Operating Systems
  - Networking
  - Applications



- Linkage between Infrastructure Networks
  - Telecommunications
  - Transportation
  - Power

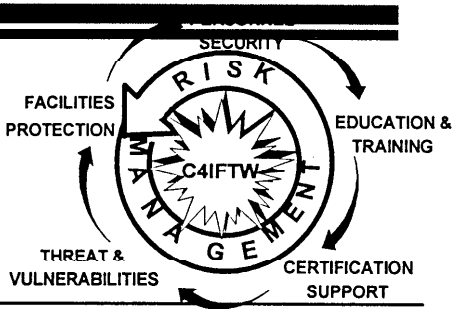




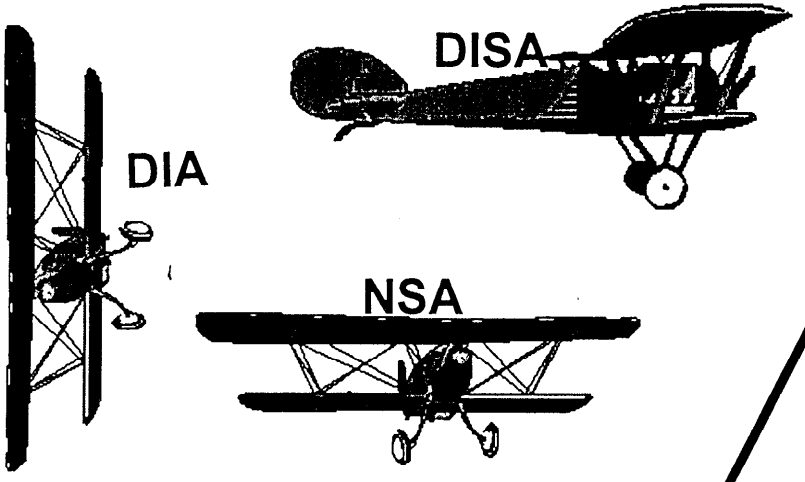
- Operating Vulnerabilities
  - Detection
  - Reporting
  - Response
- System Security Management Vulnerabilities
- User Awareness
- Policy/Procedure Adherence

Standard Certification Process

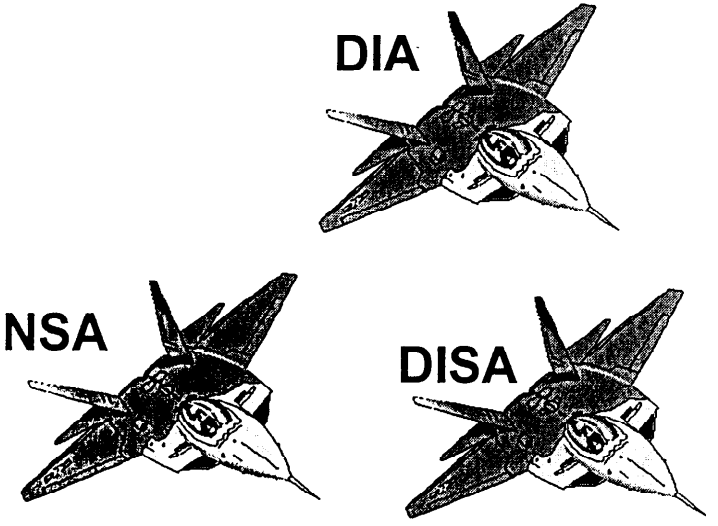
DITSCAP: DOD Information Technology Security Certification and Accreditation Process



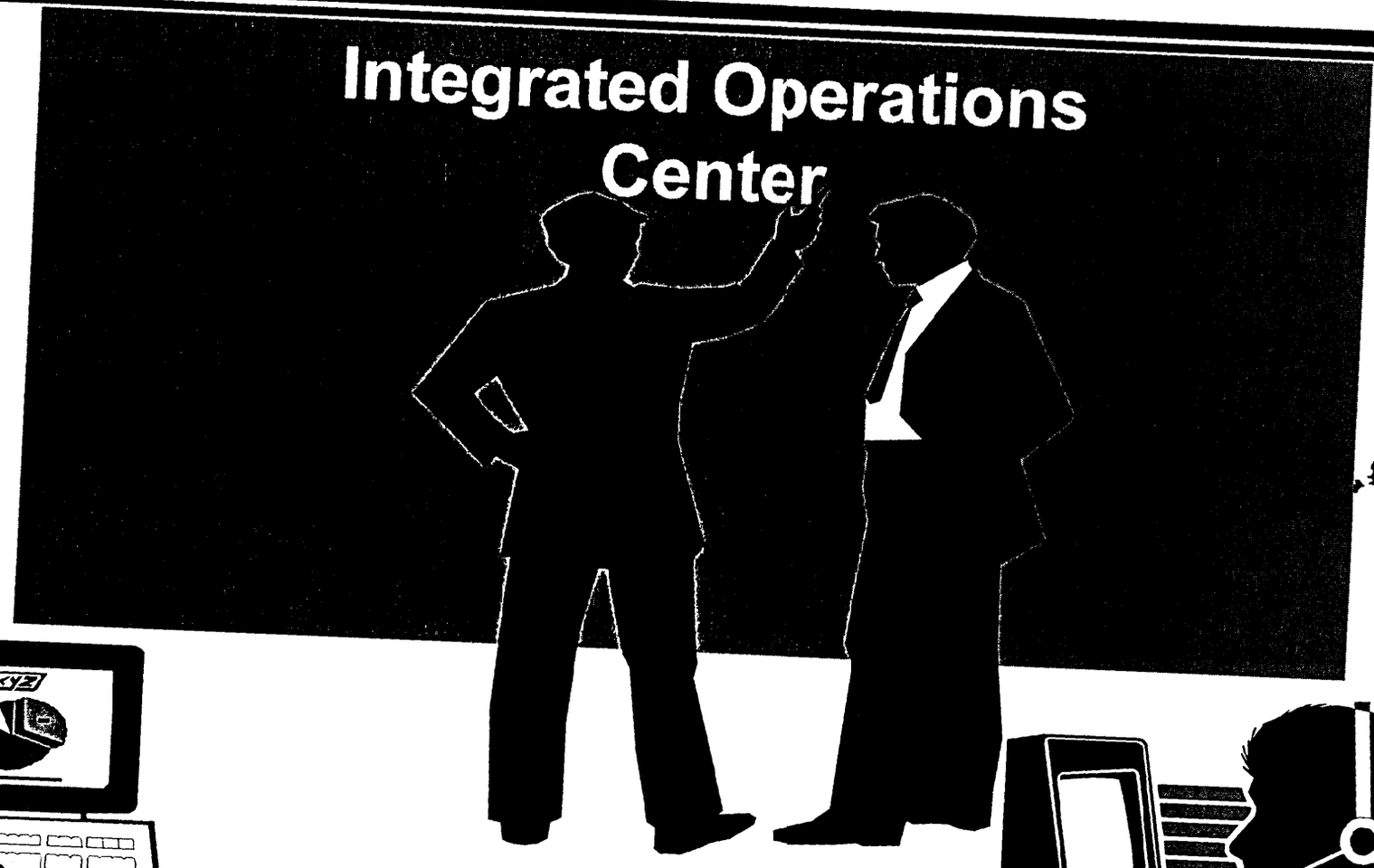
Current: System-Centric



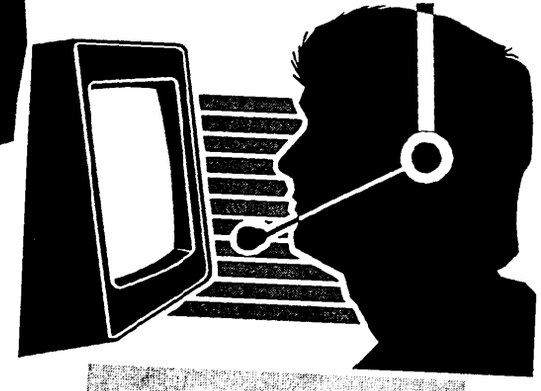
DITSCAP: Infrastructure-Centric



Current Operations

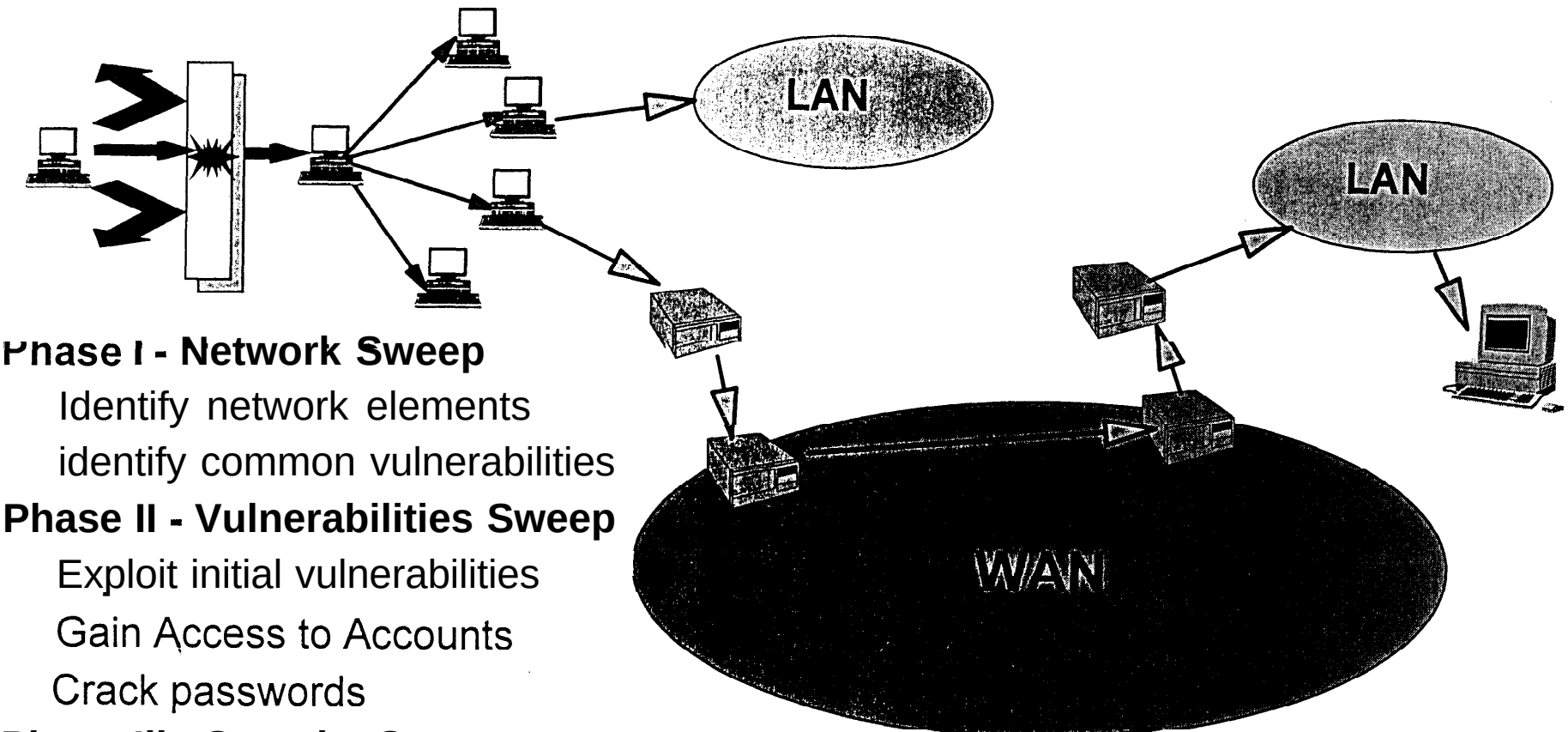


Network Ops



ASSIST

Vulnerability Assessments



Phase I - Network Sweep

Identify network elements

identify common vulnerabilities

Phase II - Vulnerabilities Sweep

Exploit initial vulnerabilities

Gain Access to Accounts

Crack passwords

Phase III - Security Sweep

Attain Greater Access

install Trojan Horses

Exploit trusted relationships

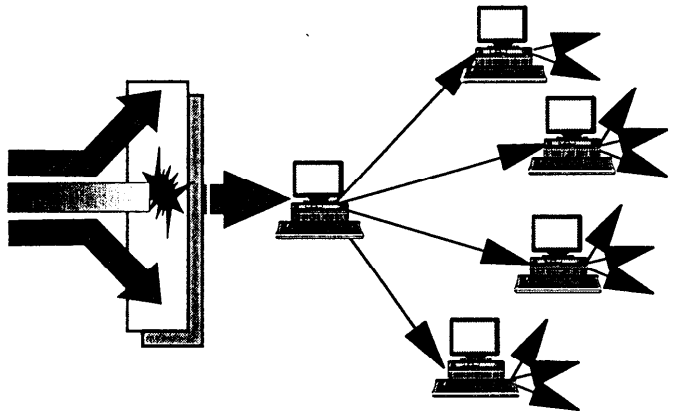
Exploit network vulnerabilities

Current Focus on UNIX and TCP/IP

Vulnerability Analysis & Assistance Program Findings

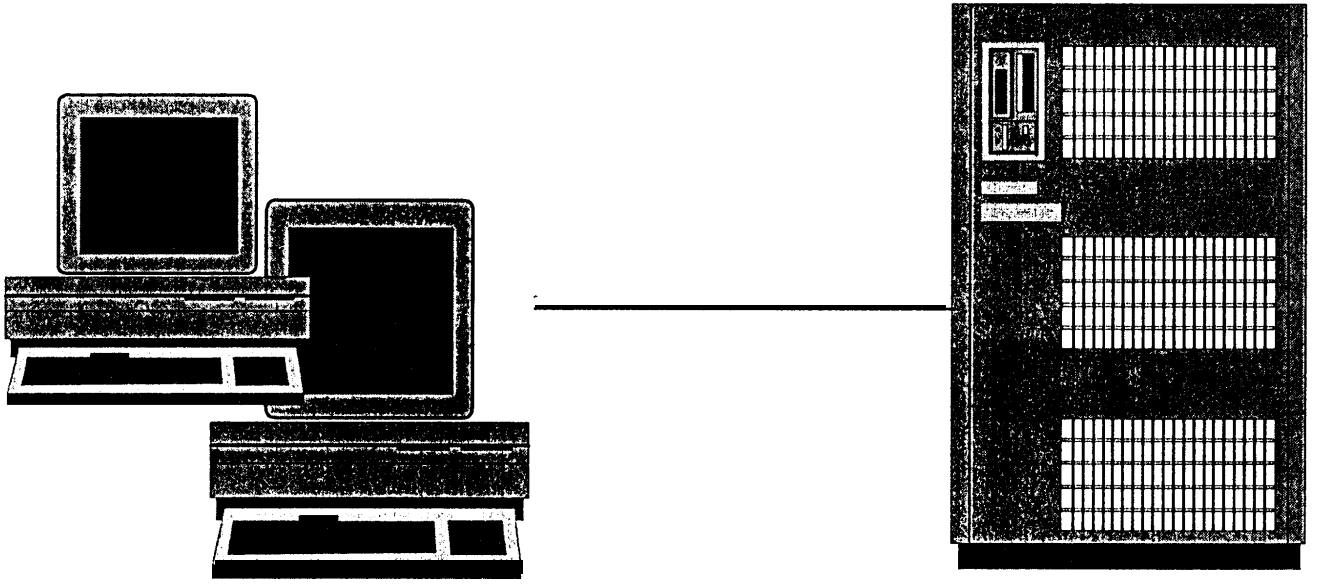
Based on 77 assessments on 38,726 Host Computers:

- 4.4% of DOD unclassified computers tested have “easily” exploitable front doors
- 65% - 89% of DOD unclassified computers tested can be further penetrated by network trusted relationships (not an indication of overall health of DII)
  - 96% of VAAP penetrations undetected by host administrators and users
    - 73% of detected penetrations go unreported



As of Oct 5, 1996

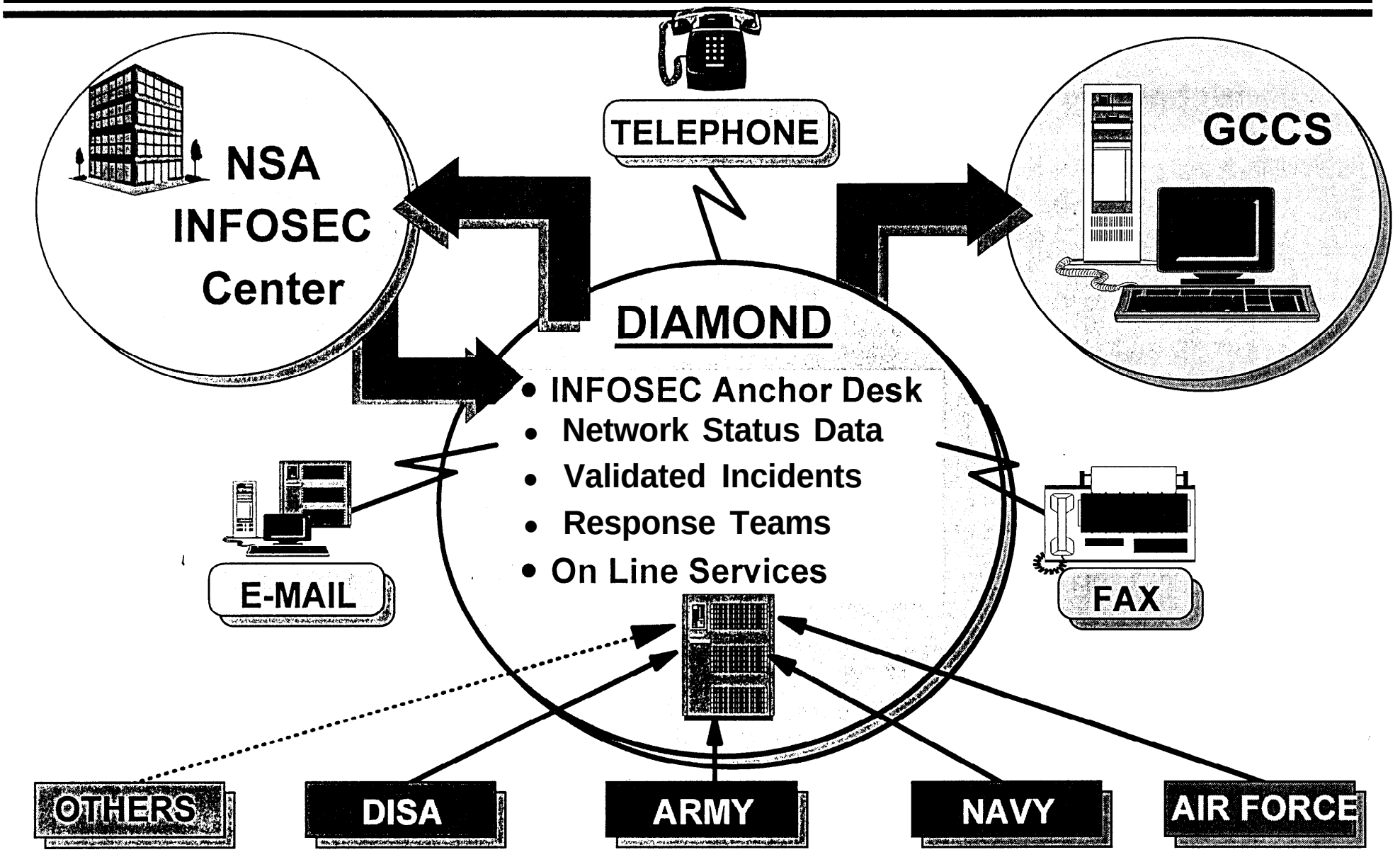
Defense in Depth: Avoid a Single Point of Failure



Connecting Lan: D○ the Hosts pass the Vulnerability Sweep?

Firewalls:Do they meet the security and operational requirements?

Defense Intrusion Analysis and Monitoring Desk (DIAMOND)

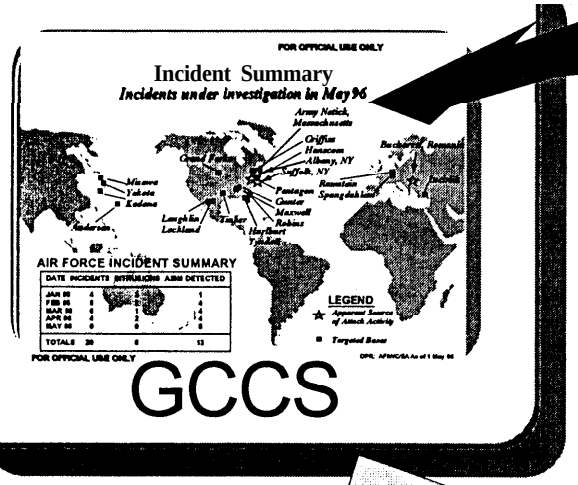


Intrusion Detection Capability

28 Sites Planned

GCC
RCCs
DMCs
DCTF
NIPRNet Gateways

Malicious Code
Data Streams
Unauthorized
Logons

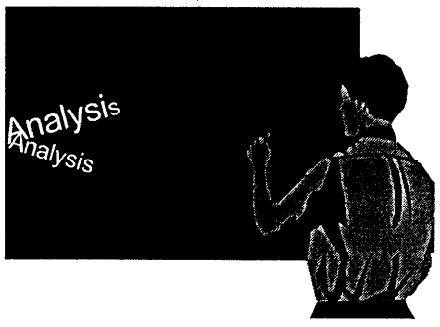


GCCS

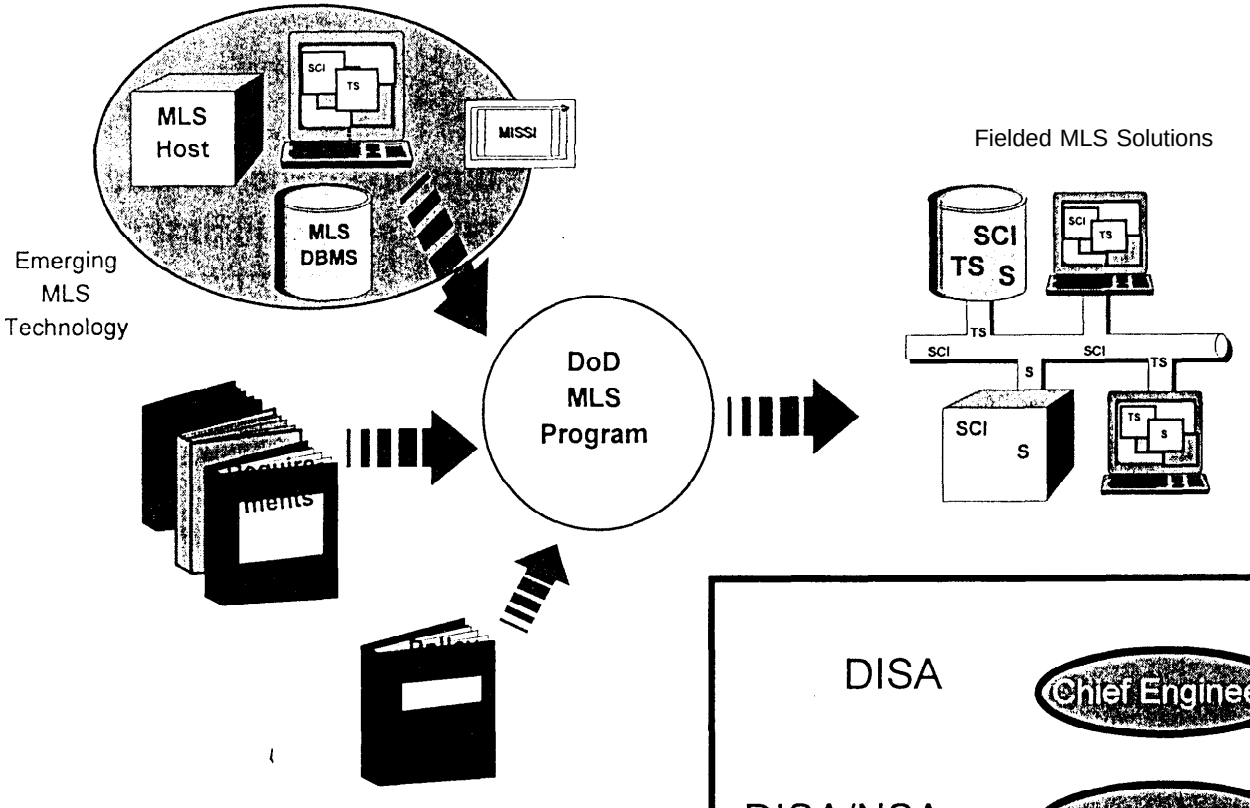
Validated Intrusions

Gold Report

Estimate 1000 Suspect Intruder Sessions Every 24 Hours on DISA's NID System Monitoring NIPRNet Fixed East Gateway

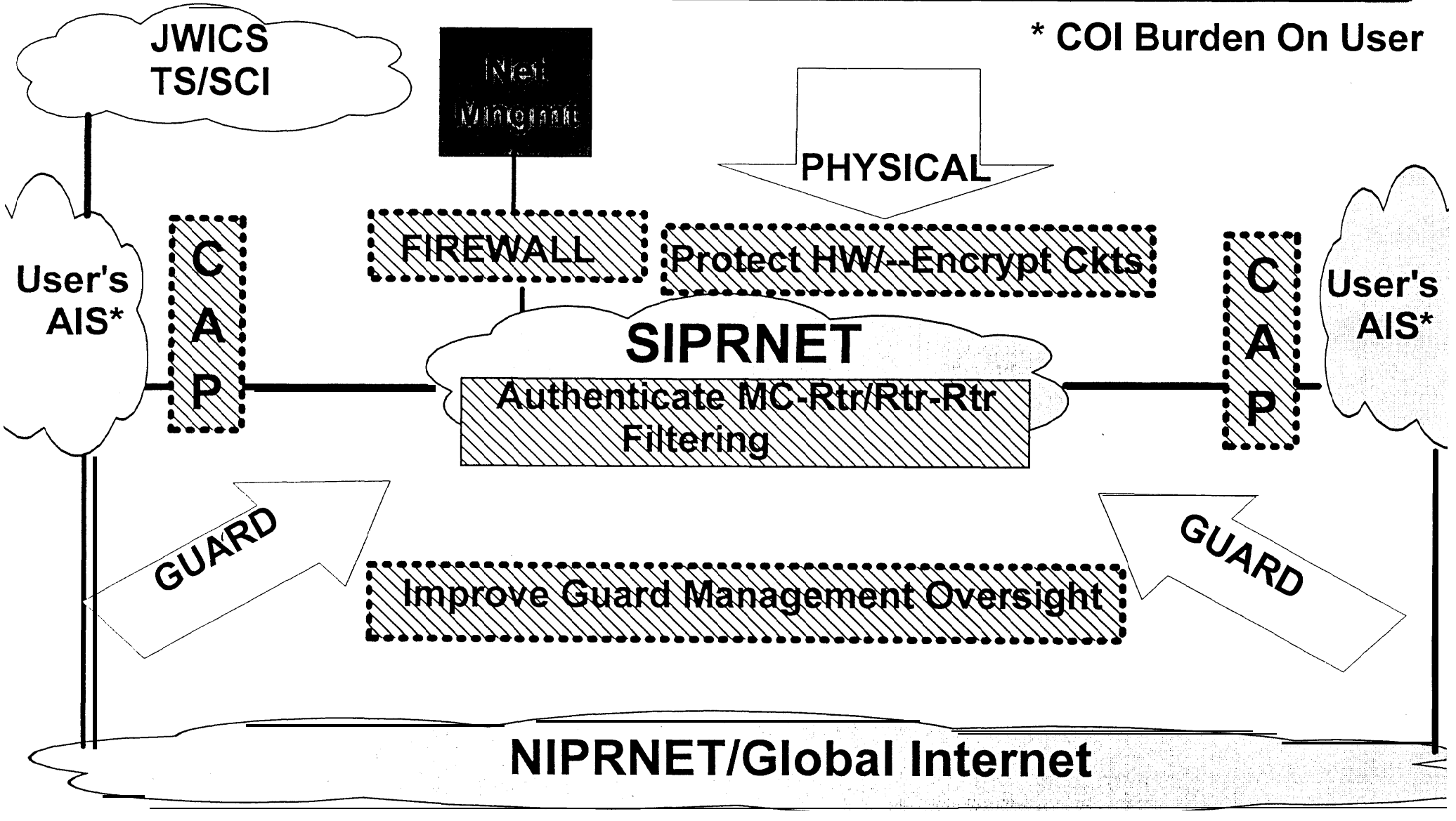


INFOSEC Engineering & DOD MLS Program



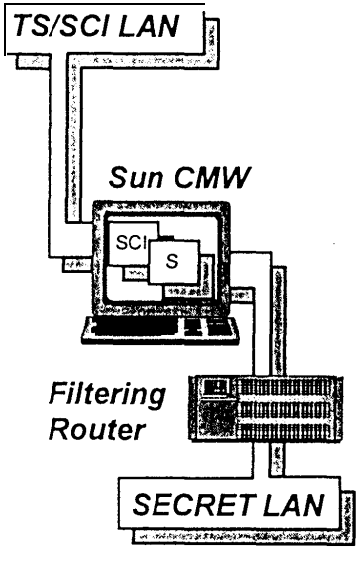
DISA	Chief Engineer	Chief Engineer	Chief Engineer
DISA/NSA	SSE Team	SSE Team	SSE Team
DISA/NSA	Other NSA & DISA INFOSEC Resources (e.g., Subject Area Expertise, Contracts, Funding)		

Network Protection

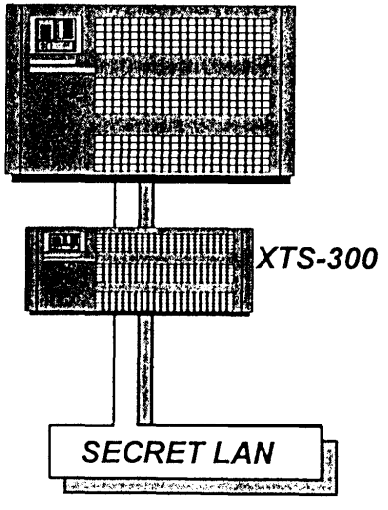


Current Security Products

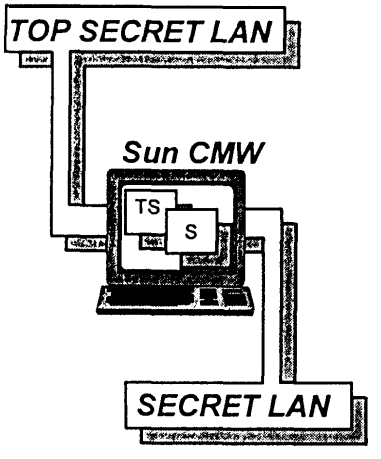
Ops/Intel Interface



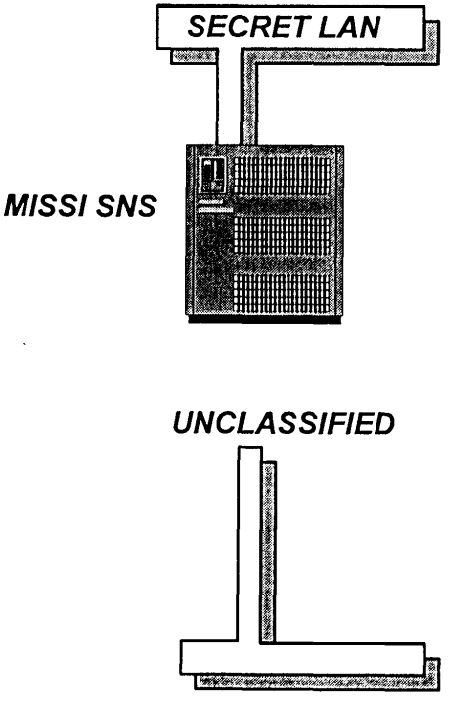
C2 Guard



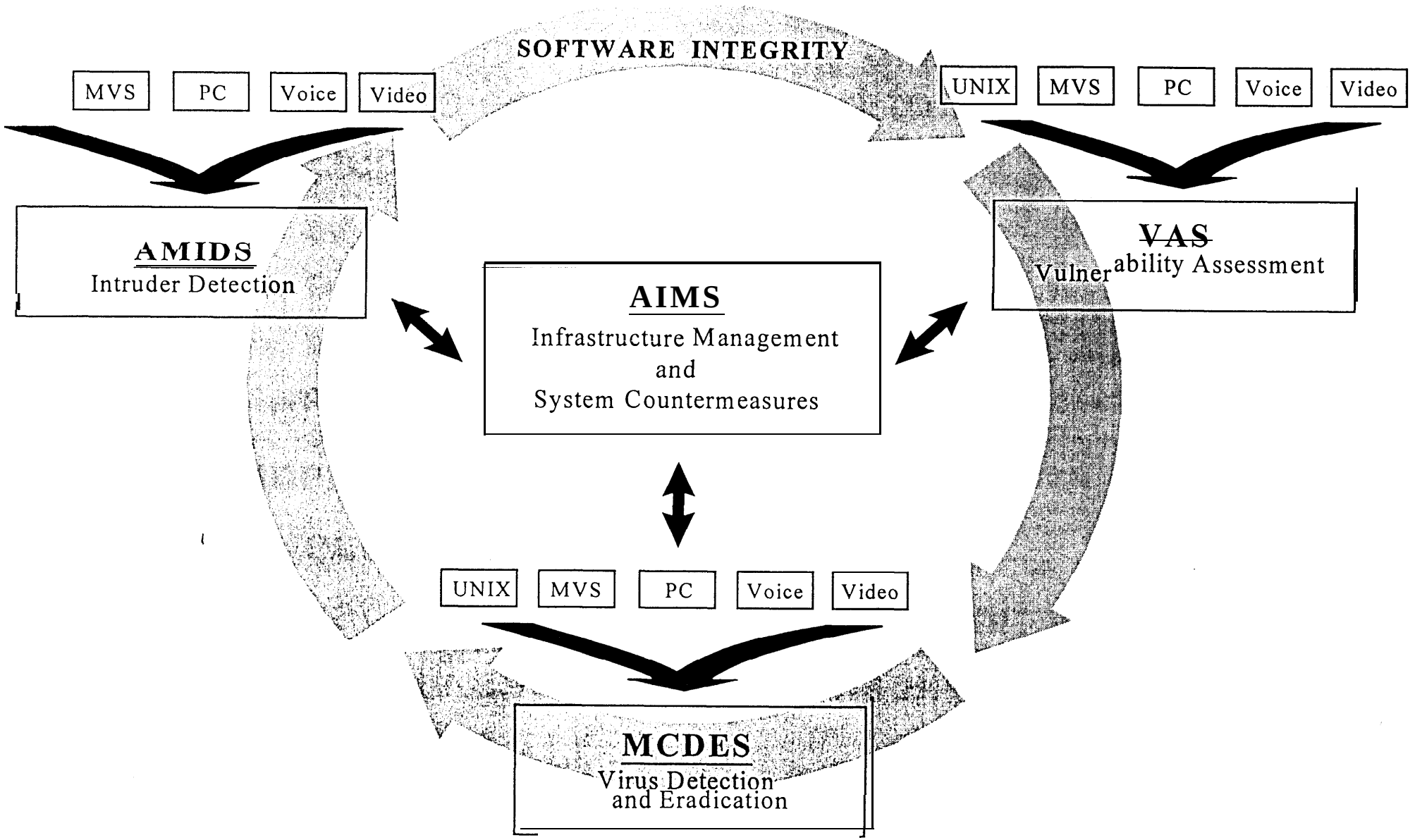
Two-Level Workstation



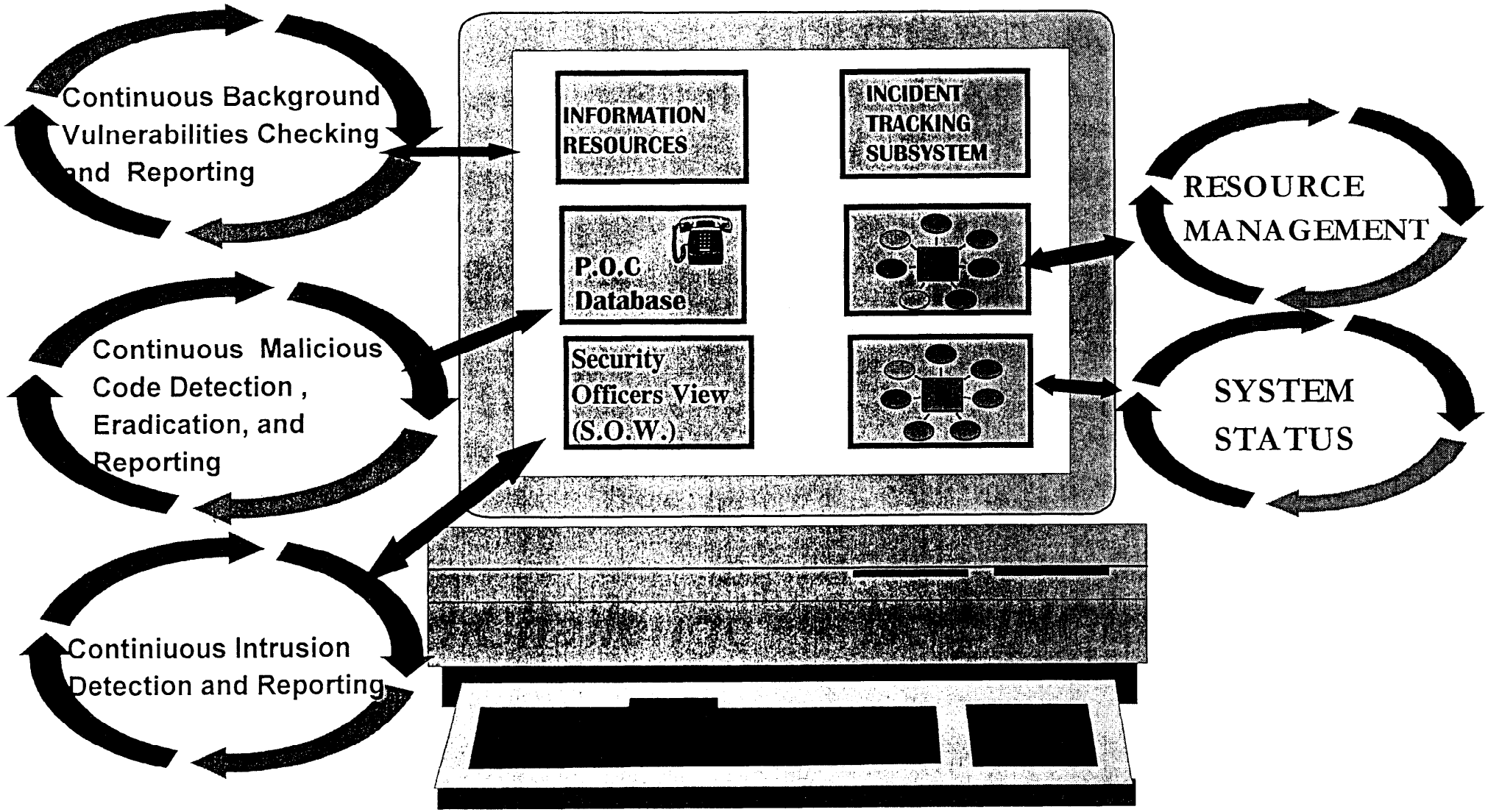
Standard Mail Guard



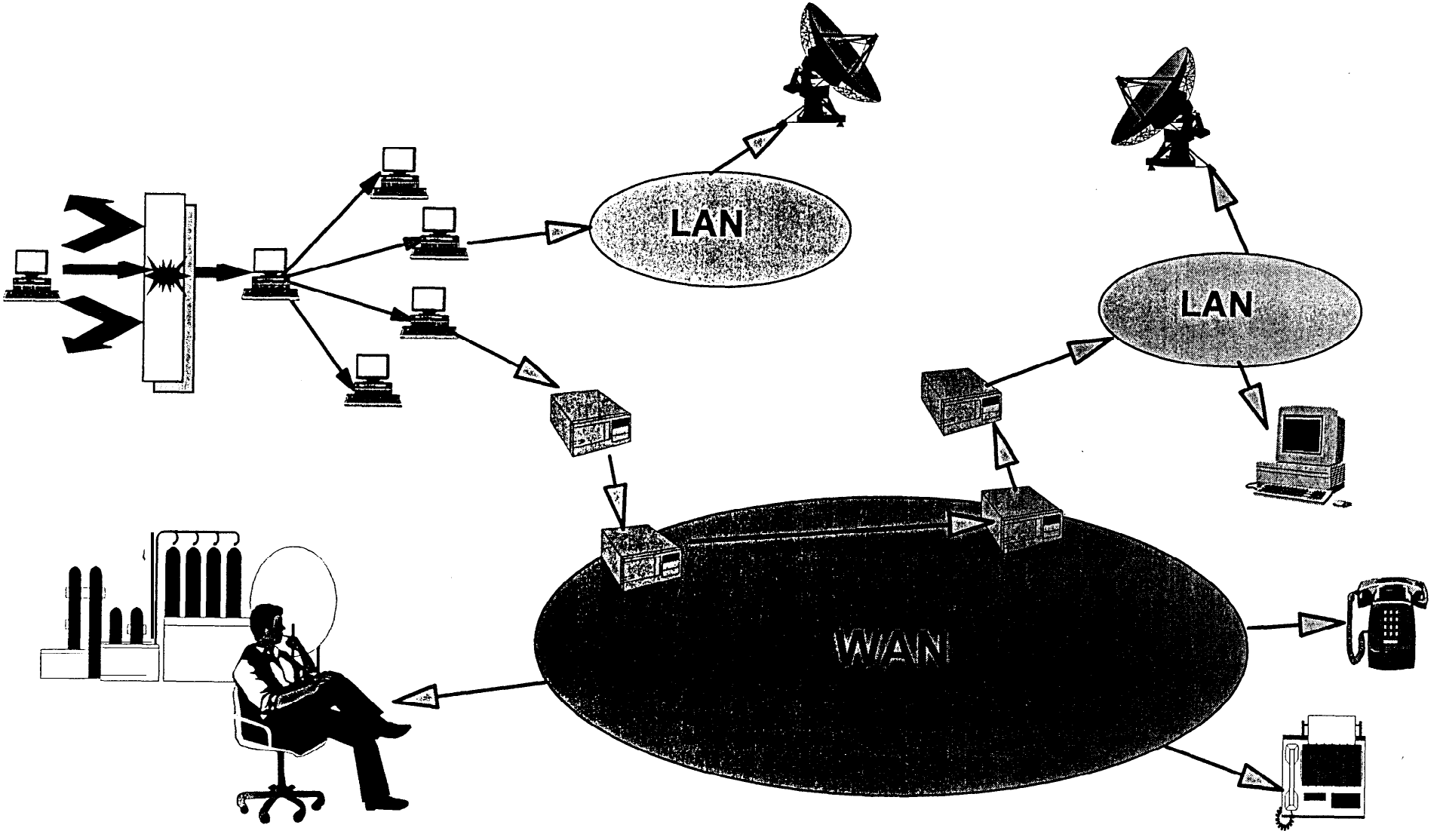
Tools: How Do they Fit Together



Automated Infrastructure Management System



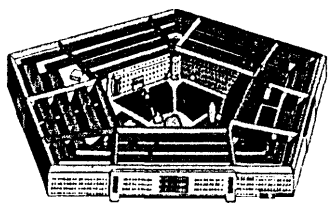
Managing Vulnerability Assessments: Integrated Tools & Red Teams

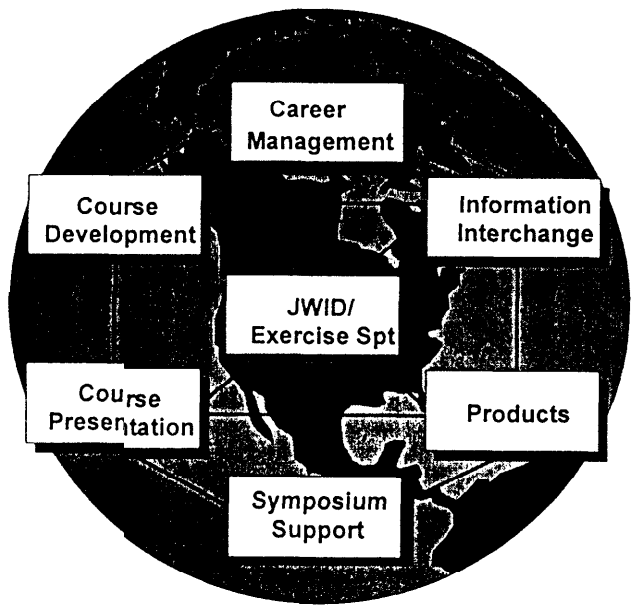


INFOSEC Education, Training &Awareness

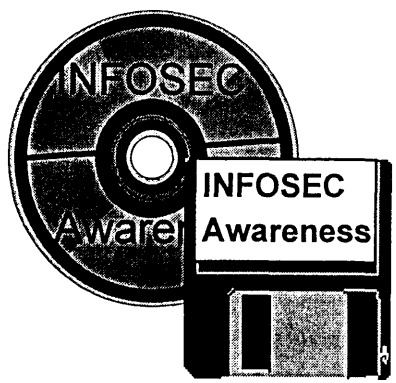
Mission:

- Courseware Development and Delivery
- INFOSEC Awareness Products
- INFOSEC Professional Development





DISSPatch

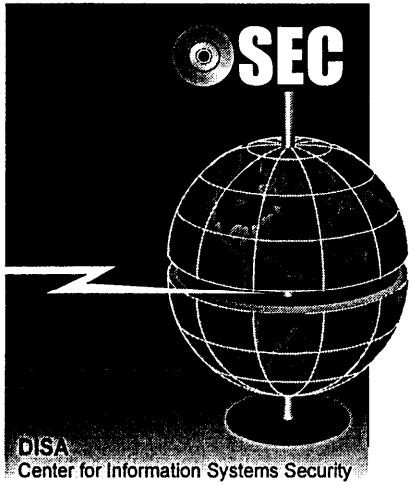


INFOSEC Technical Services Contract

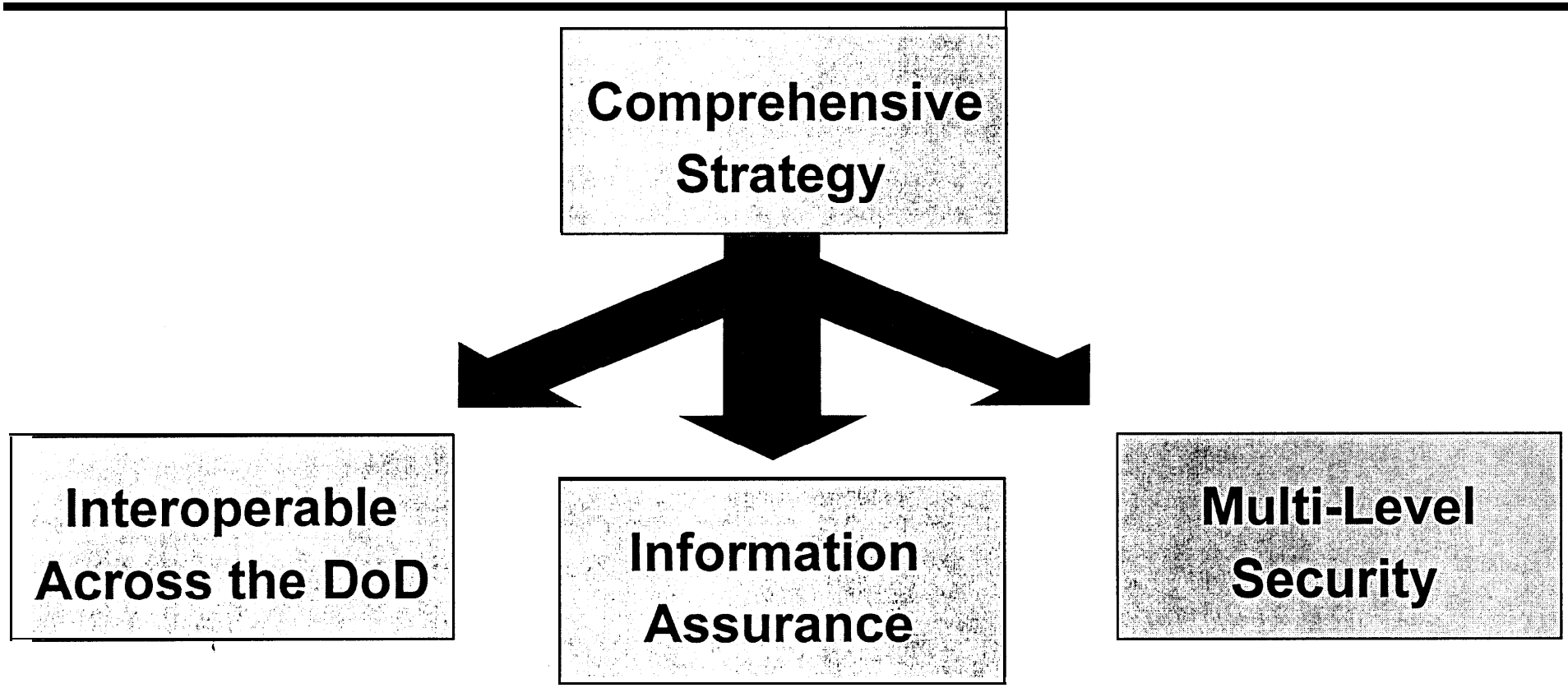
- Quick reaction contract support to DOD **&** other Federal Departments/Agencies

- Three Contractor Teams

- Areas of Support Include:
  - Engineering
  - Architecture
  - Certification, evaluation and accreditation
  - Vulnerability assessment tools and techniques
  - Training and Awareness



Summary: The Way Ahead



Multifaceted Challenge - - No SINGLE Solution