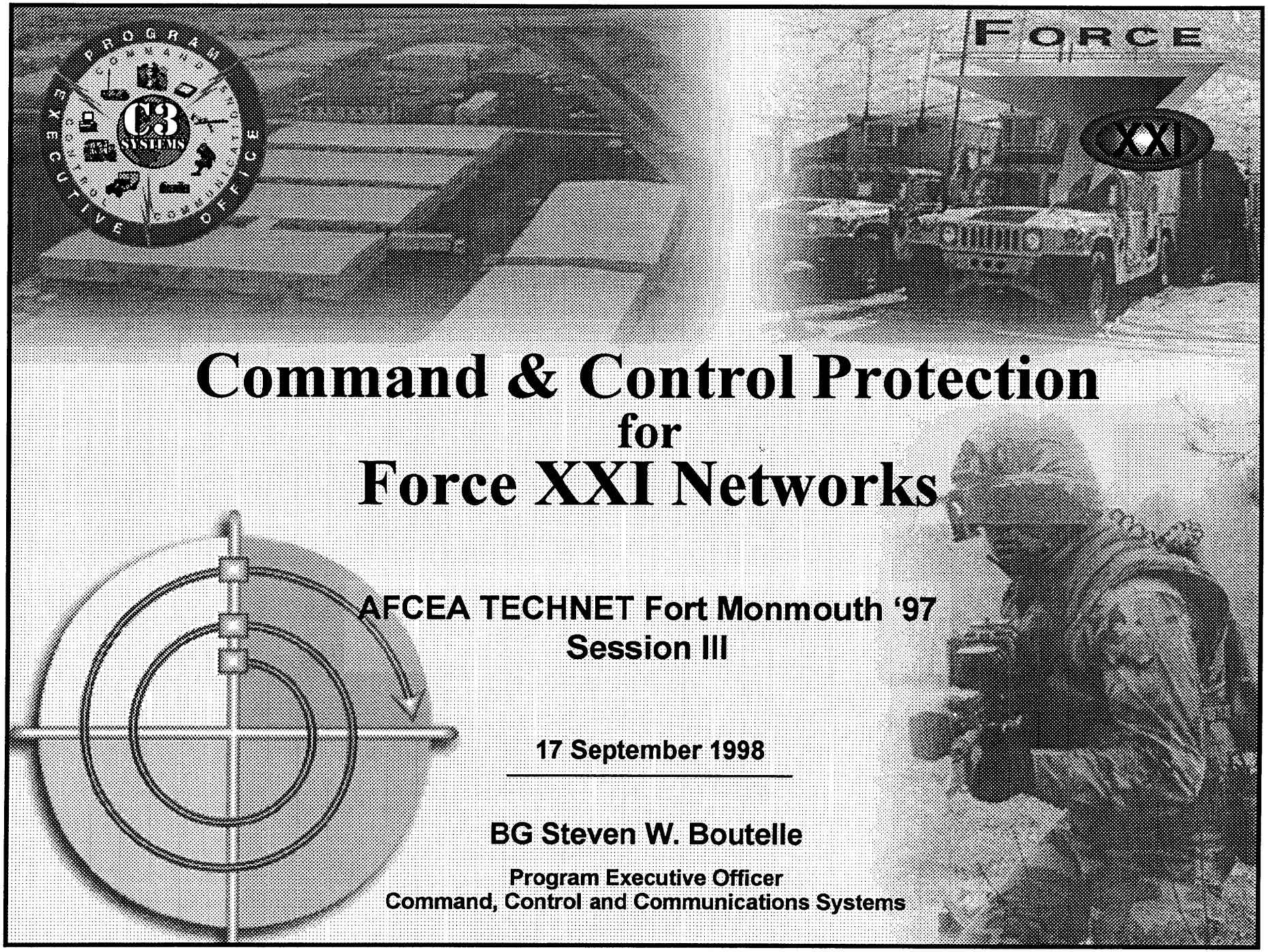


Command & Control Protection for Force XXI Networks

AFCEA TECHNET Fort Monmouth '97
Session III

17 September 1998

BG Steven W. Boutelle
Program Executive Officer
Command, Control and Communications Systems

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01091992	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Command & Control Protection for Force XXI Networks	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Information Assurance Technology Analysis Center (IATAC) 3190 Fairview Park Drive Falls Church VA 22042	**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 18	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	9/1/92	Briefing

4. TITLE AND SUBTITLE
Command & Control Protection for Force XXI Networks

5. FUNDING NUMBERS

6. AUTHOR(S)
Not provided

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Information Assurance
Technology Analysis Center
(IATAC)
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-AI
8725 John J. Kingman Road,
Suite 944

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This briefing, on the Command and Control Protection for Force XXI Networks presented to AFCEA TECHNET at Fort Monmouth, NJ in 1997 by the Program Executive Officer, Command, Control and Communications Systems. It provides an overview of battlefield communications, and information system security, first digitized division. It includes host based C2 protect tools, commercial off the shelf (COTS) tools, as well as FBCB2 Security Policy.

14. SUBJECT TERMS

15. NUMBER OF PAGES

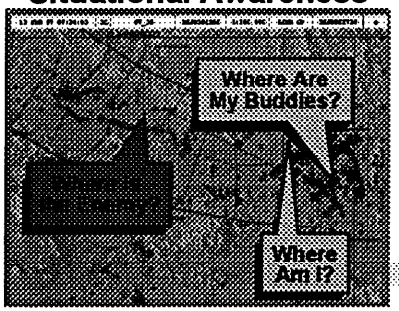
16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited

Digitization Is A Key Enabler To Gaining Information Dominance

FASTER MORE ACCURATE DECISIONS
TO INFLUENCE THE BATTLEFIELD
ENABLED BY INFORMATION DOMINANCE

Dominant Maneuver thru Situational Awareness



DISTRIBUTES SITUATIONAL AWARENESS INFORMATION RAPIDLY

Dominant Maneuver thru Collaborative Planning

PROVIDES THE GBR WITH THE ABILITY TO DISTRIBUTE INTENT/ORDERS QUICKLY

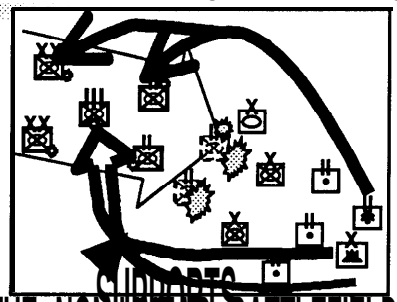
Precision Engagement

MOVE SENSOR TO SHOOTER INFORMATION RAPIDLY

Focused Logistics

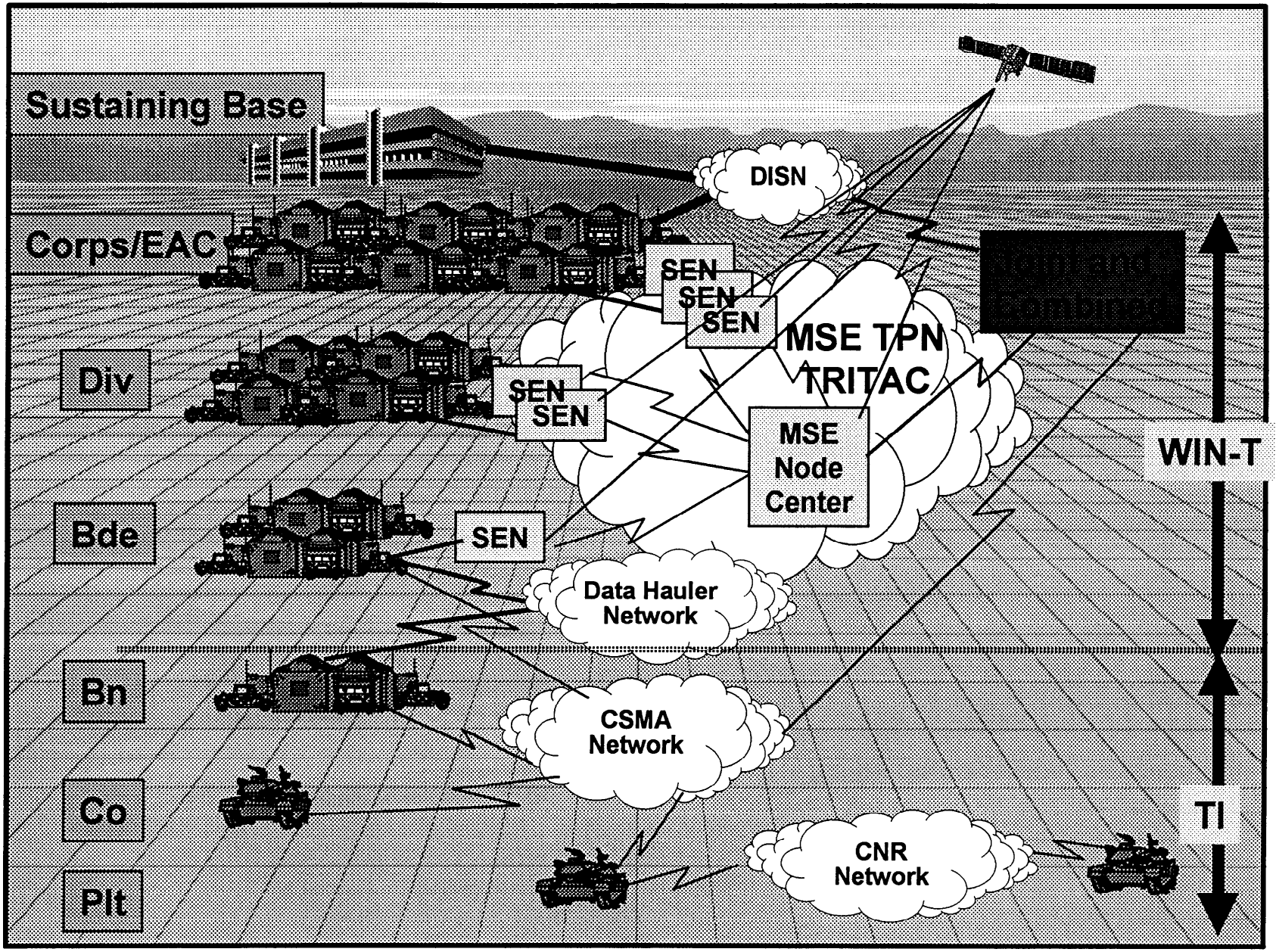
PROVIDES SUPPORT TO ANTICPATORY LOGISTICS

Dominant Maneuver thru Greater Mobility & Flexibility



SUPPORTS THE NON-LINEAR BATTLEFIELD

Battlefield Communications Overview



Information System Security

Challenge

Provide commanders and their staff with information that is:

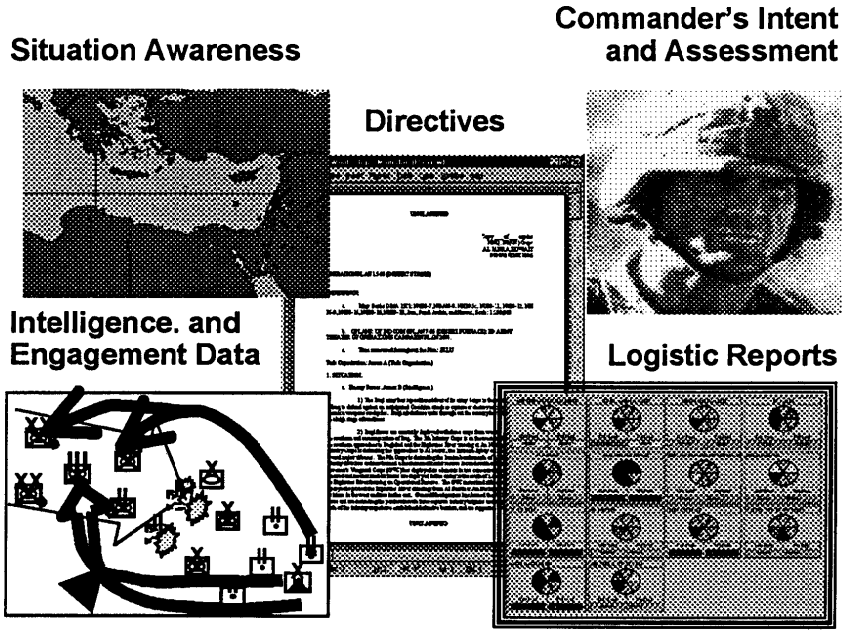
- **Timely**
- **Accurate**
- ***SECURE***
- **Performance and Security Balanced**

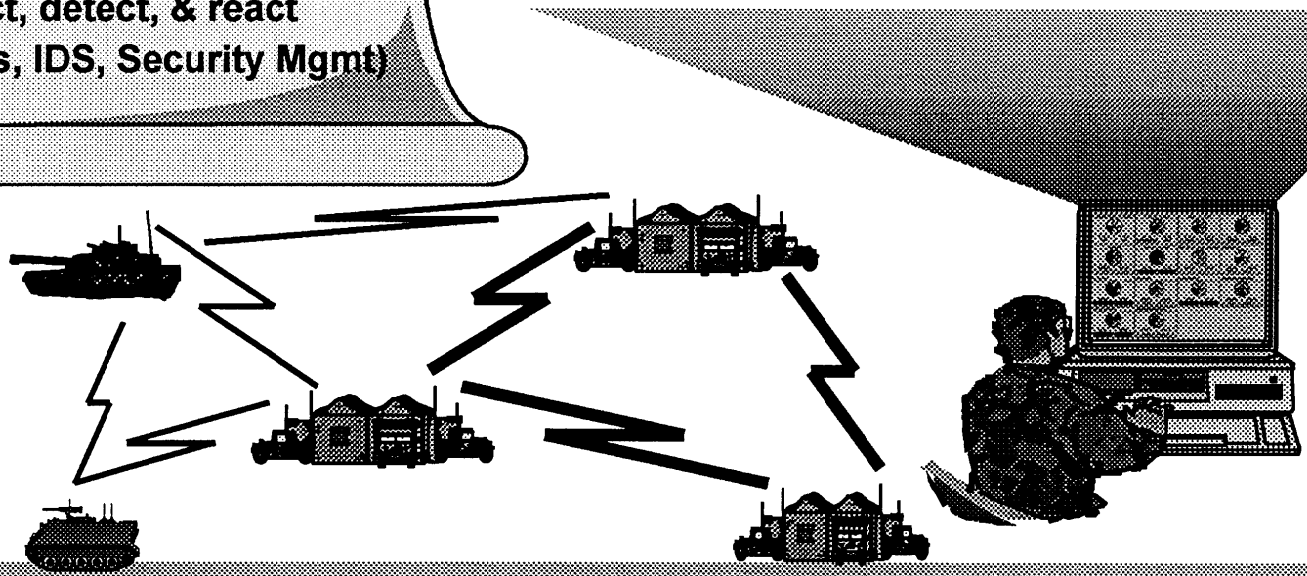
(THESE ARE ALL PROTECTION REQUIREMENTS!!!)

Command and Control Protection Tenets

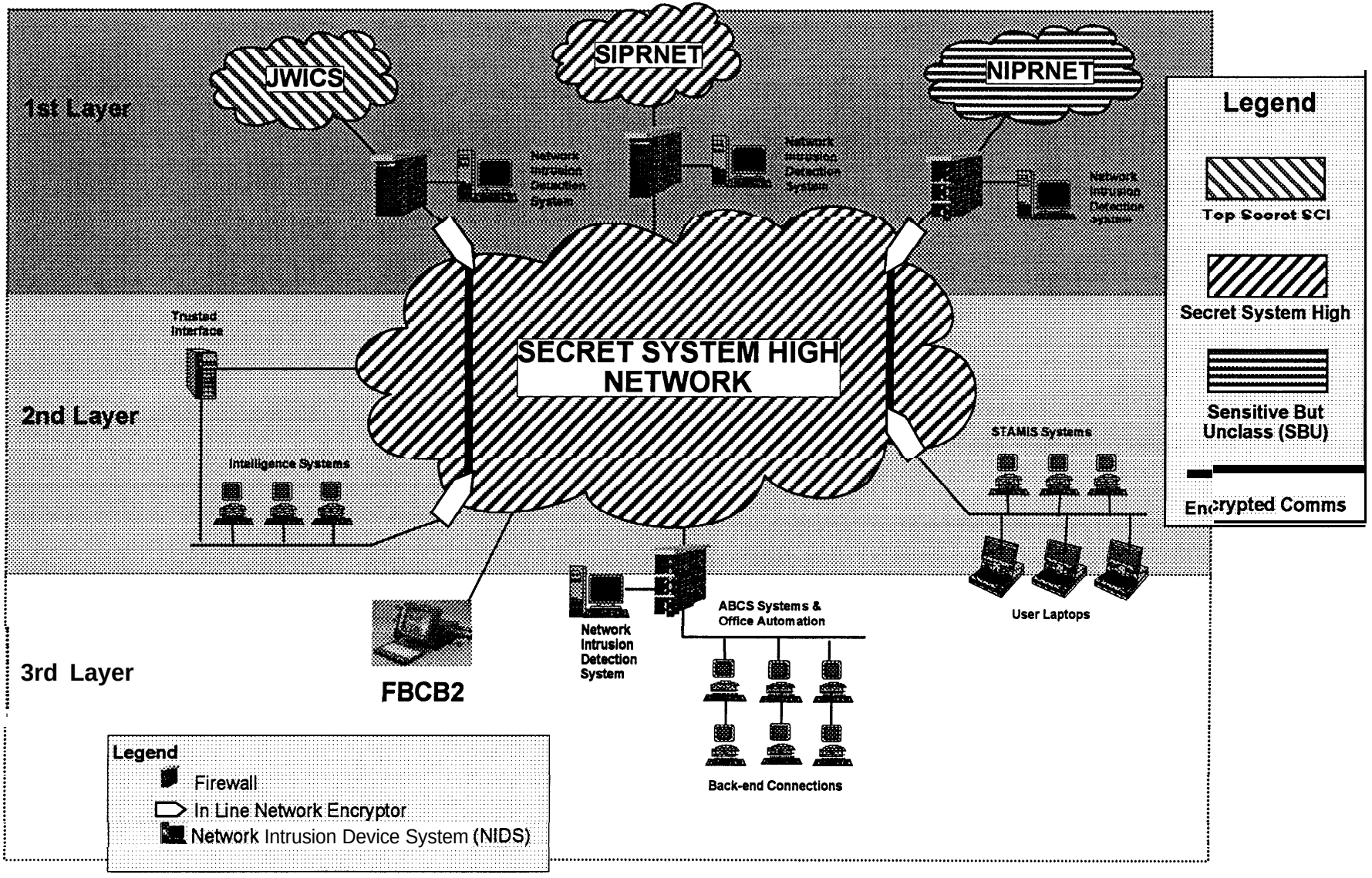
- **Defense in depth**
- **Protect, detect, & react**

(C2P Tools, IDS, Security Mgmt)



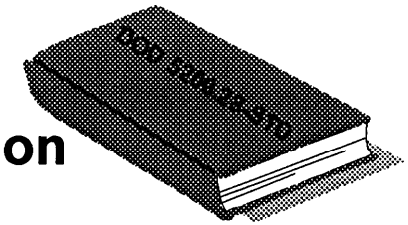


First Digitized Division (FDD) Security Architecture



Host-Based C2 Protect

- **Hosts Systems**
  - **As a minimum, all host systems will meet DOD 5200.28-STD Class C2 Protection Level Requirements**



  - **All hosts systems will incorporate network authentication, integrity, and access control mechanisms in accordance with the Army C2 Protect Program**
  - **Hosts systems will incorporate intrusion detection functionality to extent possible/practical**
- **Applications**
  - **Strong authentication, integrity, access control and non-repudiation mechanisms as required per service**

Goal is to implement common C2 Protect tools for all ABCS systems

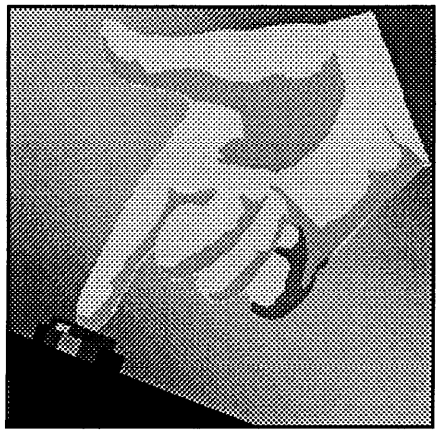
Host-Based C2 Protect Tools

- TCP Wrappers to protect transaction
- Security Profile Inspector (SPI) to maintain configuration
- SWATCH to alert on audit anomalies

- Network Associates Anti-Virus
- Password Checkers

Currently installed on all ABCS systens

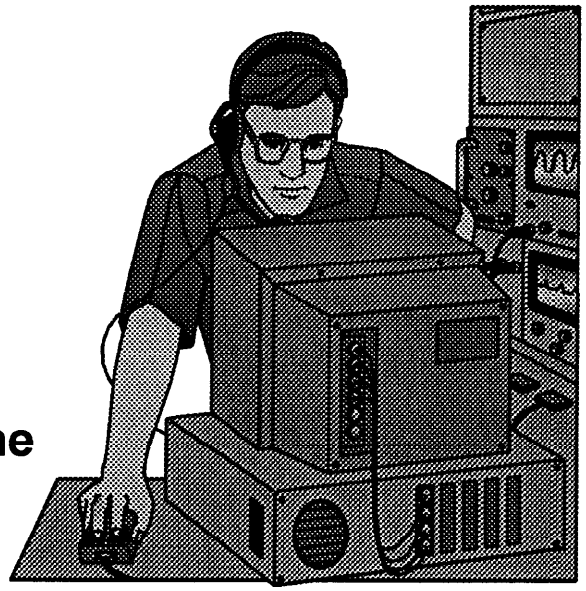
Current "Commercial Off The Shelf' (COTS) Integration Efforts



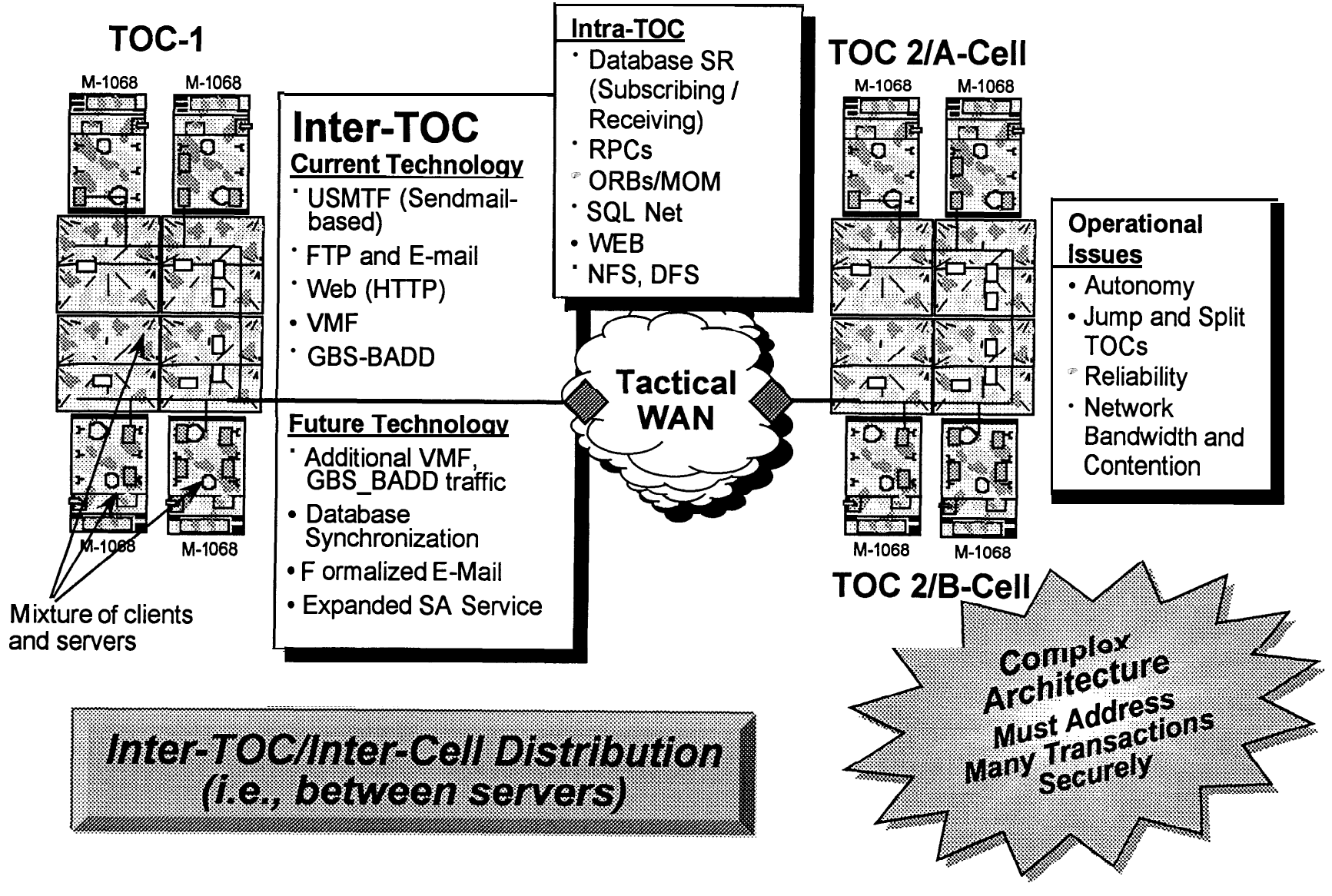
- **Purge Routines**
  - **Reviewing/evaluating products available for complete memory purge to transition workstations between classified and unclassified roles**

- **Secure Client - Server Services**
  - **Reviewing/evaluating products that can provide**
    - **Authentication**
    - **Encryption**

  in the multiple DCE cell environment of the Tactical Operations Center



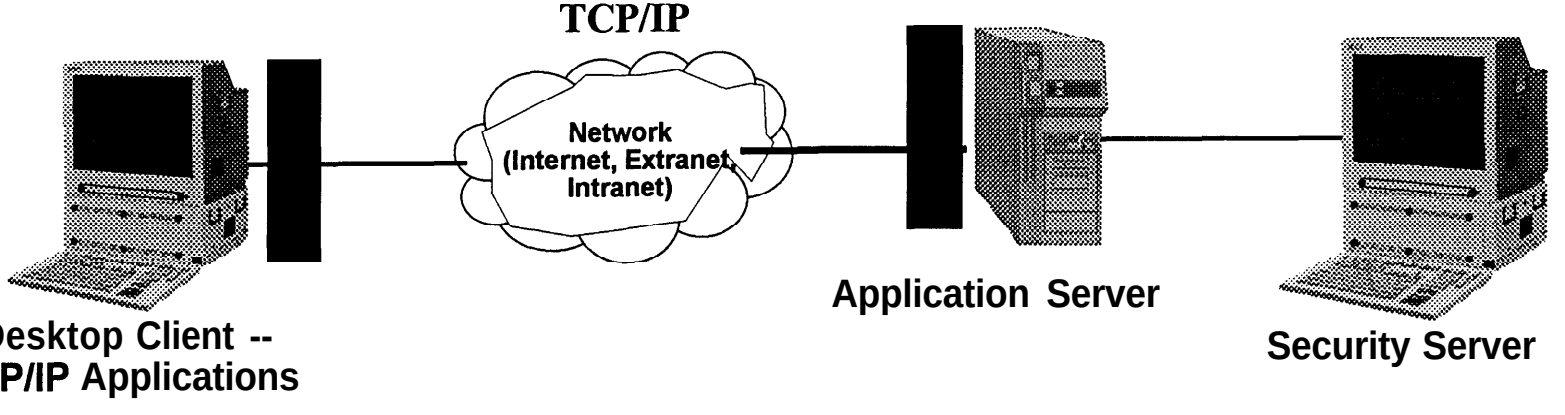
Inter-TOC and Intra-TOC Data Distribution



Inter-TOC/Inter-Cell Distribution (i.e., between servers)

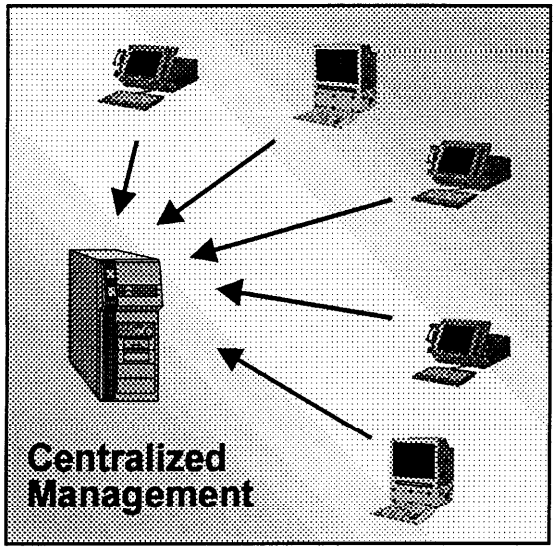
COTS Example

- **Combines the strengths of Secret Key and Public Key encryption technologies**
- **Provides comprehensive security framework for all TCP/IP based applications**
  - **Includes single sign-on . . . in a completely transparent manner**



COTS Secure Capabilities

- **Authentication and single sign-on**
- **Standardized authorization across all applications**
- **Data protection services, smart Virtual Private Network (VPN)**

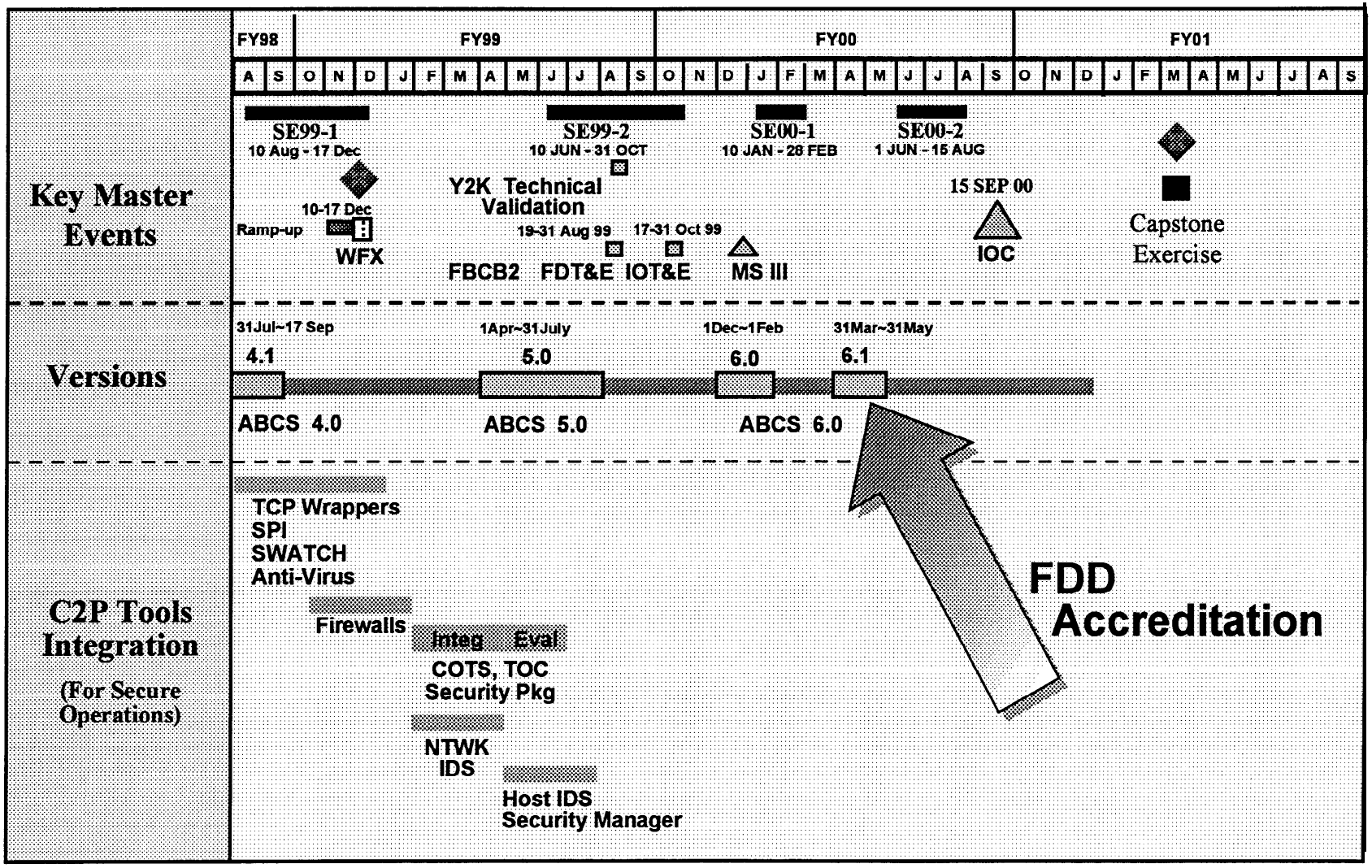


- **Dynamic support for new protocols**
- **Centralized management, connection monitoring**
- **Auditing, accounting, event notification**

- **Public key certificate services**

C2 Protect Integration

Master FDD Schedule (Version 1.3)



FBCB2 Initial Protection Capabilities
Oct '99

- FBCB2 authenticates to the router upon request to grant/validate network access
- Access control to data based on clearance level
  - Clears C2 data when operational level lowered to SBU
- Capability for any user to initiate both disk overwrite and resetting of the router to factory default
- Audit reports generated and forwarded to designated collection points

FBCB2: Force XXI Battle Command Brigade and Below

FBCB2 Capabilities Planned for FDD
Sep '00

- **Remote security management**
  - **Load passwords**
  - **Control system access: three operational capabilities**
    - **. Challenge a user to re-authenticate without interfering with the mission**
    - **. Lock-out the user until re-authentication**
    - **. Disable - through overwrite of the disk and reset of the router to its factory default**
  - **Authentication through the use of digital signature**
    - **. Security management transactions initiated/signed by security manager and sent to remote FBCB2**
- **Ongoing evaluation of C2 Protection enhancements**
  - **Message authentication, intrusion detection, malicious code detection**

FBCB2: Force XXI Battle Command Brigade and Below

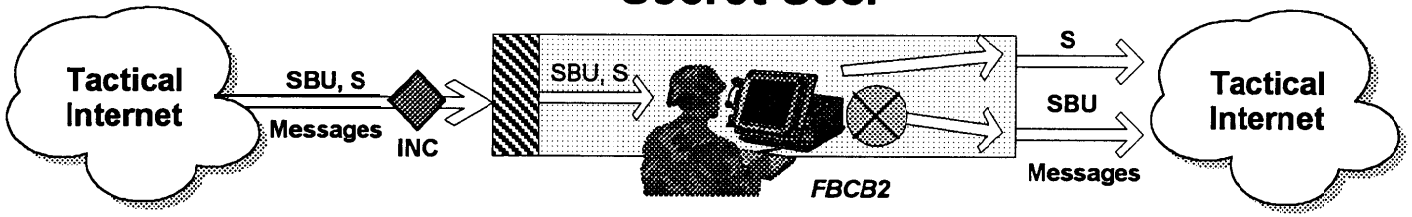
Summary FBCB2 Security Policy

Each Computer Maintains a SECRET System High Posture
Discretionary Access Control (DAC) of SECRET Data is Enforced at End-Points

At Sending End -
Manual review required for message remark

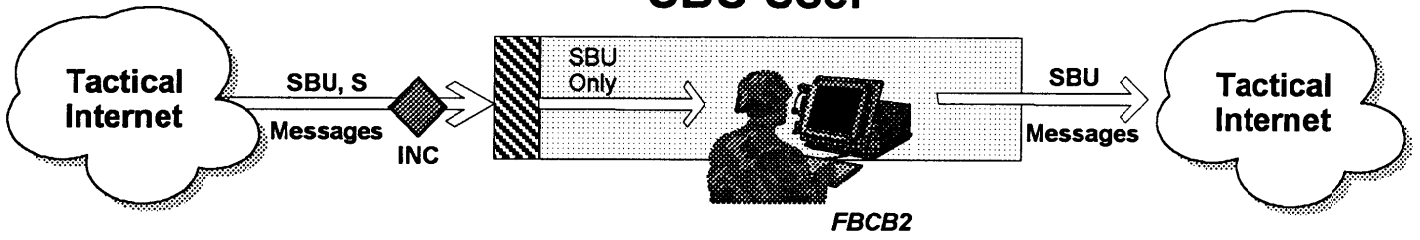
At Receiving End -
Hard rejection of messages marked above User level

Secret User



Human Review and "Remark"

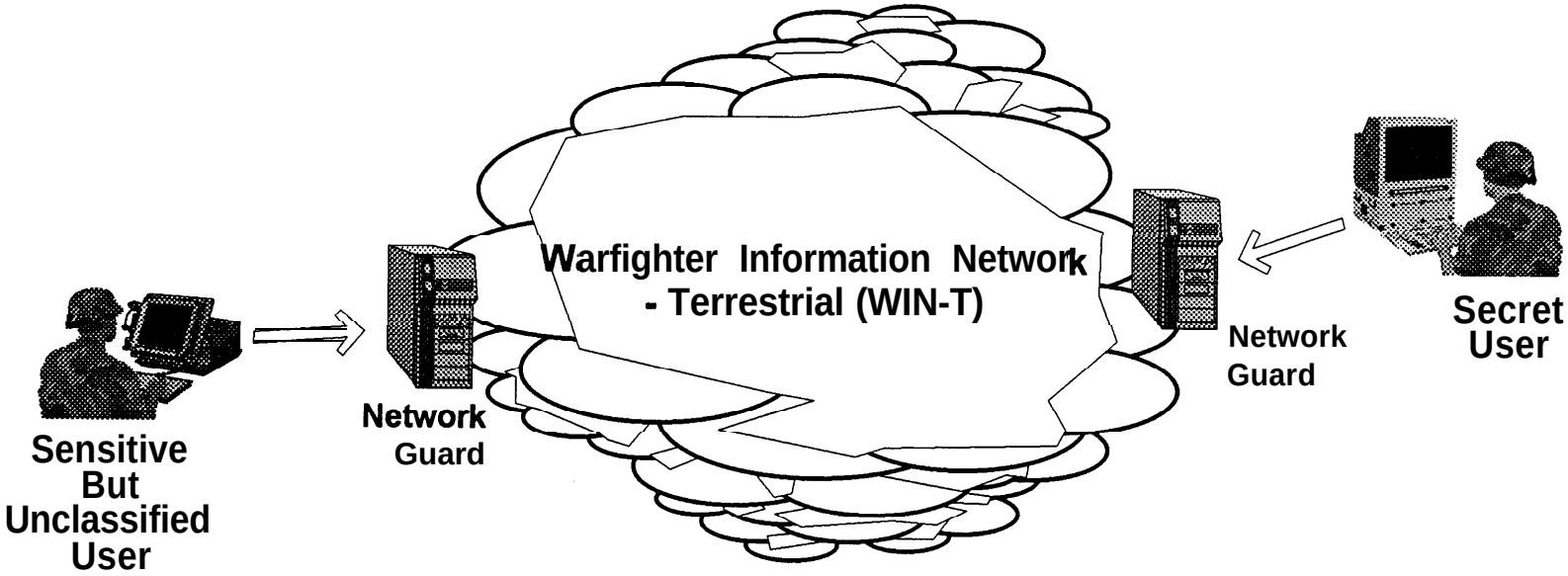
SBU User



Legend
Message Rejection | Message Remarked | SBU Sensitive But Unclassified | S Secret

Future Force XXI C2P

- **Selective Purge**
- **Host Intrusion Detection Systems**
- **Tactical network guards to allow information exchange automatically between classification levels**



Summary

- **Information Assurance (IA) is a proactive and imperative part of the Army Digitization Program**
- **PEO C3S PMs will continue to aggressively pursue emerging assurance technologies, e.g.**

-Smart cards for user authentication

Biometrics for Access Control

- Biometrics for access control

- Personal / host-level firewalls

- . . . .