NETWORK SECURITY IMPROVEMENT PROGRAM

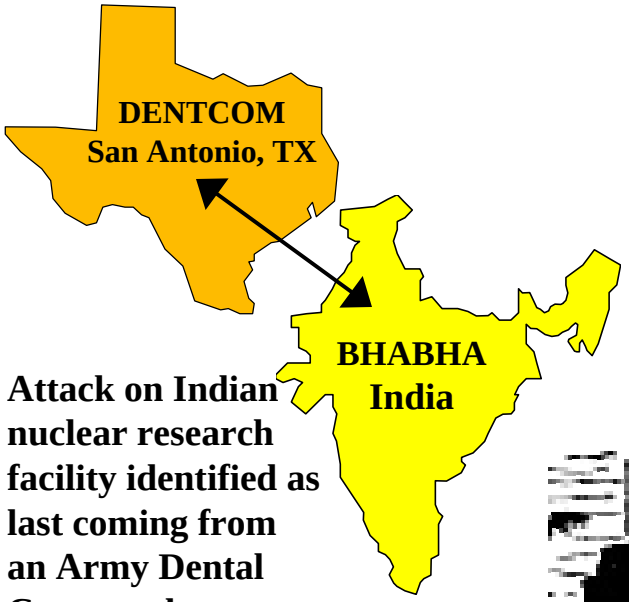
Director of Information Systems for Command, Control, Communications, and Computers

Secretary of the Army
Information Assurance Division

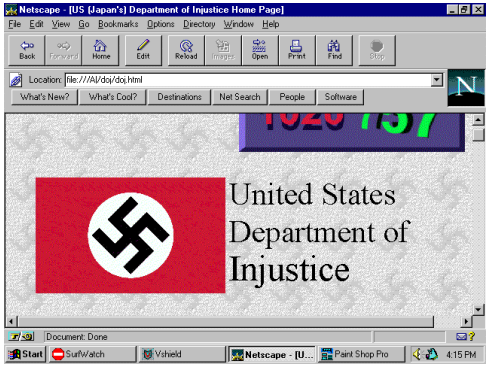
Mr. Philip Loranger
703-607-5886
loranjp@hqda.army.mil

LTC LeRoy Lundgren
703-604-8377 (DSN 664)
lundgl@hqda.army.mil

CONSEQUENCES OF BEING VULNERABLE TO THE THREAT



Attack on Indian nuclear research facility identified as last coming from an Army Dental Command system



Loss of Public Confidence

e.g., apparent inability to protect publicly accessible web sites

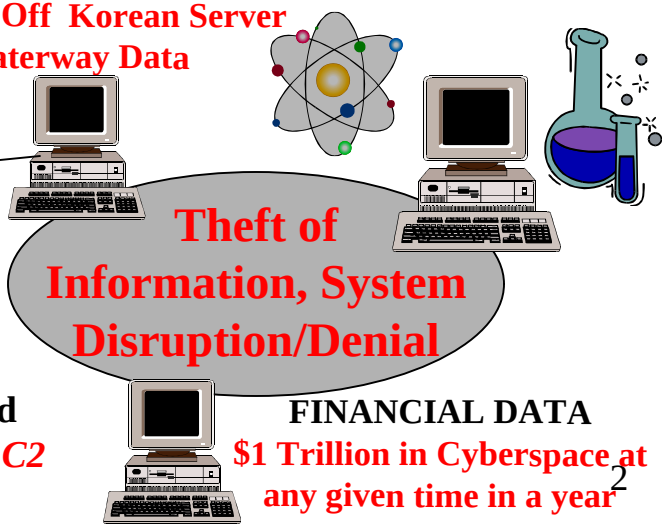
Potential International Repercussions

Unprotected Backdoor into network

Intruder able to search files at will, control the Command's network, and potentially *control the Commander's C2*

STOLEN PLANS & PROGRAMS
MSC Technology by Jenot
SECRET Data Off Korean Server
COE Waterway Data

RESEARCH LABORATORIES
ARL & DREN at Risk



Theft of Information, System Disruption/Denial

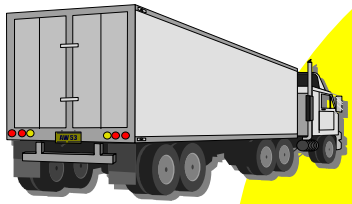
FINANCIAL DATA
$1 Trillion in Cyberspace at any given time in a year

SCOPE OF THE CHALLENGE

FINANCE

CORPS OF ENGINEERS

TRANSPORTATION



WWW sites

ARMY CIRCUITS
NON ARMY CIRCUITS
ISP CONNECTIONS
CONTRACTOR PT TO PTS
DIAL-IN SYSTEMS
FUNCTIONAL NETWORKS

E-Mail

SIDPERS

CPO

MEDICAL

INTRUDERS

WHY NSIP ?

- *Mid-February '98*
  Hackers attacked DoD Networks
  VCSA directs "fixes" at FLASH precedence

- *DEPSECDEF Directs CINCs, Services, and Agencies to achieve "positive control" over their systems and networks*

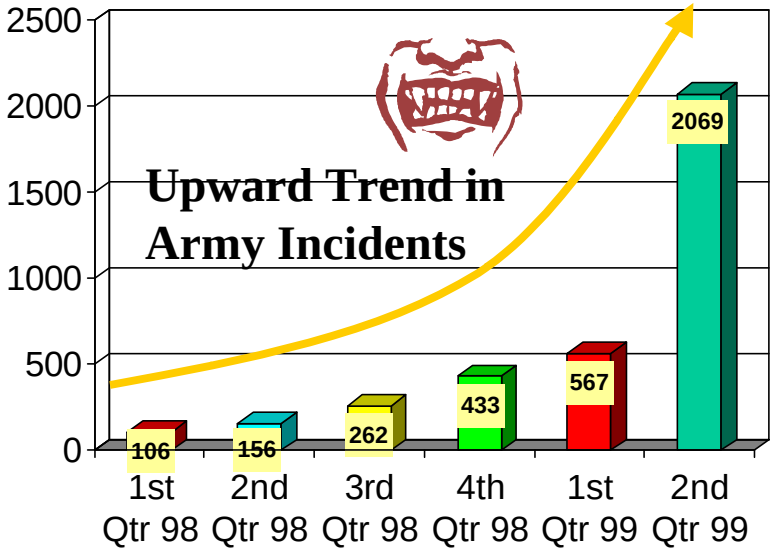
- *Army leadership directed DISC4 IA Office to formulate plans to protect the Army's Critical Infrastructure*

- *Genesis of the Army:*

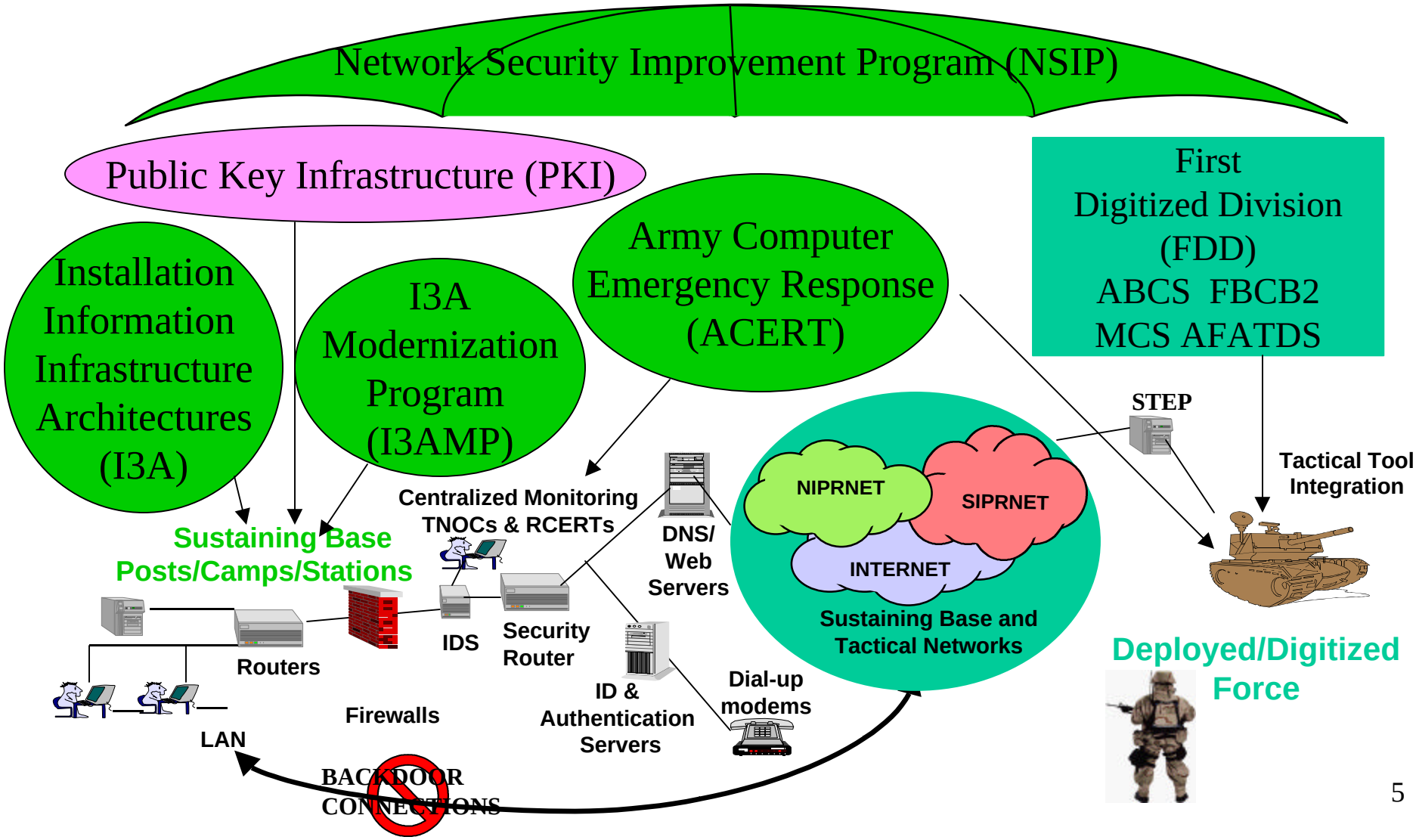
The Network Security Improvement Program

Army FY 99 Data

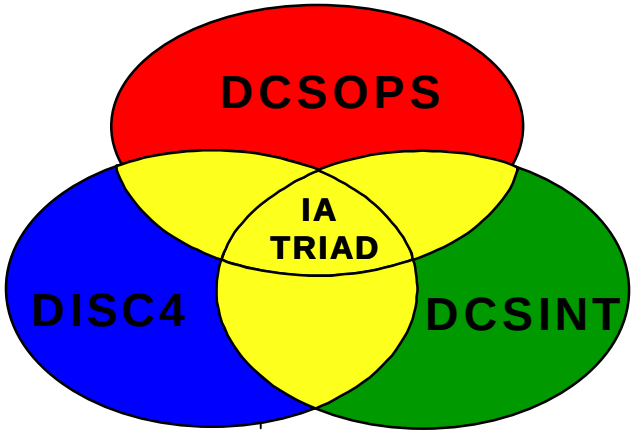
- 25M Security Events
- 2,069 Incidents
- 37 Intrusions

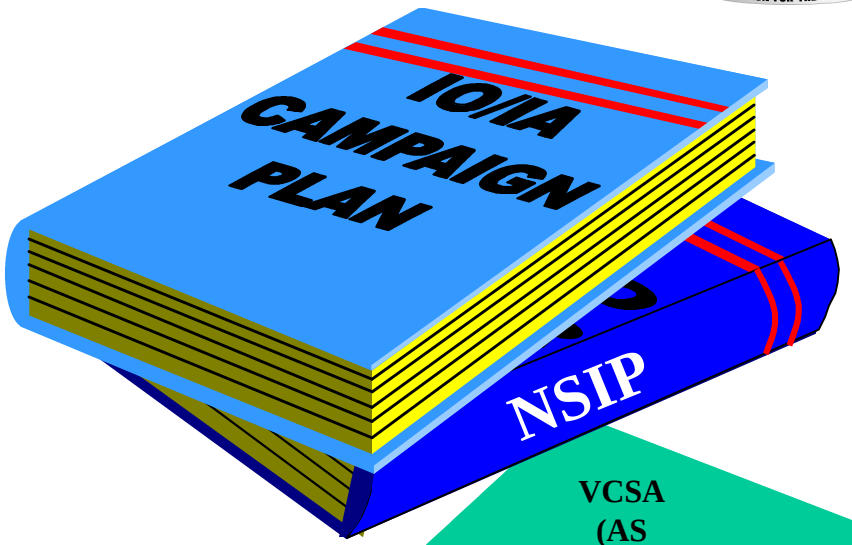


WHAT IS NSIP ?


Network Security Improvement Program (NSIP)
Public Key Infrastructure (PKI)
Installation Information Infrastructure Architectures (I3A)
I3A Modernization Program (I3AMP)
Army Computer Emergency Response (ACERT)
First Digitized Division (FDD)
ABCS FBCB2
MCS AFATDS
STEP
Tactical Tool Integration
Centralized Monitoring
TNOCs & RCERTs
Sustaining Base
Posts/Camps/Stations
DNS/
Web
Servers
NIPRNET
SIPRNET
INTERNET
Sustaining Base and
Tactical Networks
Routers
IDS
Security
Router
Firewalls
ID &
Authentication
Servers
Dial-up
modems
LAN
BACKDOOR
CONNECTIONS
Deployed/Digitized
Force

ARMY IA TEAM





Tactics, Techniques, & Procedures

Army Signal Cmd

CECOM/ISEC

Army CERTs

Input from Leadership and Field

Implementers

MACOMs/PEOs/PMs/Activities

VCSA (AS REQUIRED)

SENIOR IO REVIEW COUNCIL

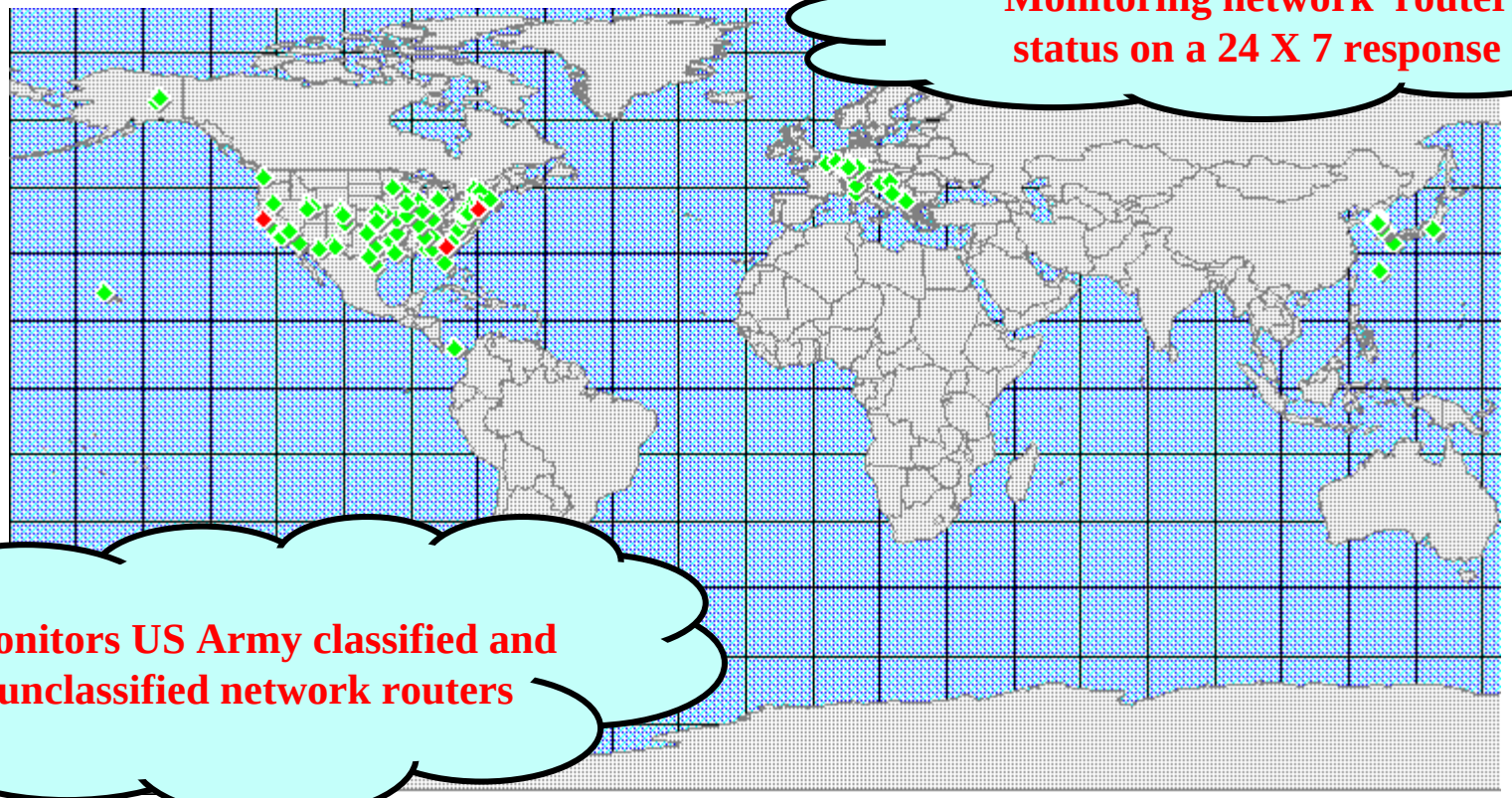
GOSC

COUNCIL OF COLONELS

NSIP PHASE I ACCOMPLISHMENTS

ACTUAL VIEW OF ARMY NETWORK ROUTER STATUS

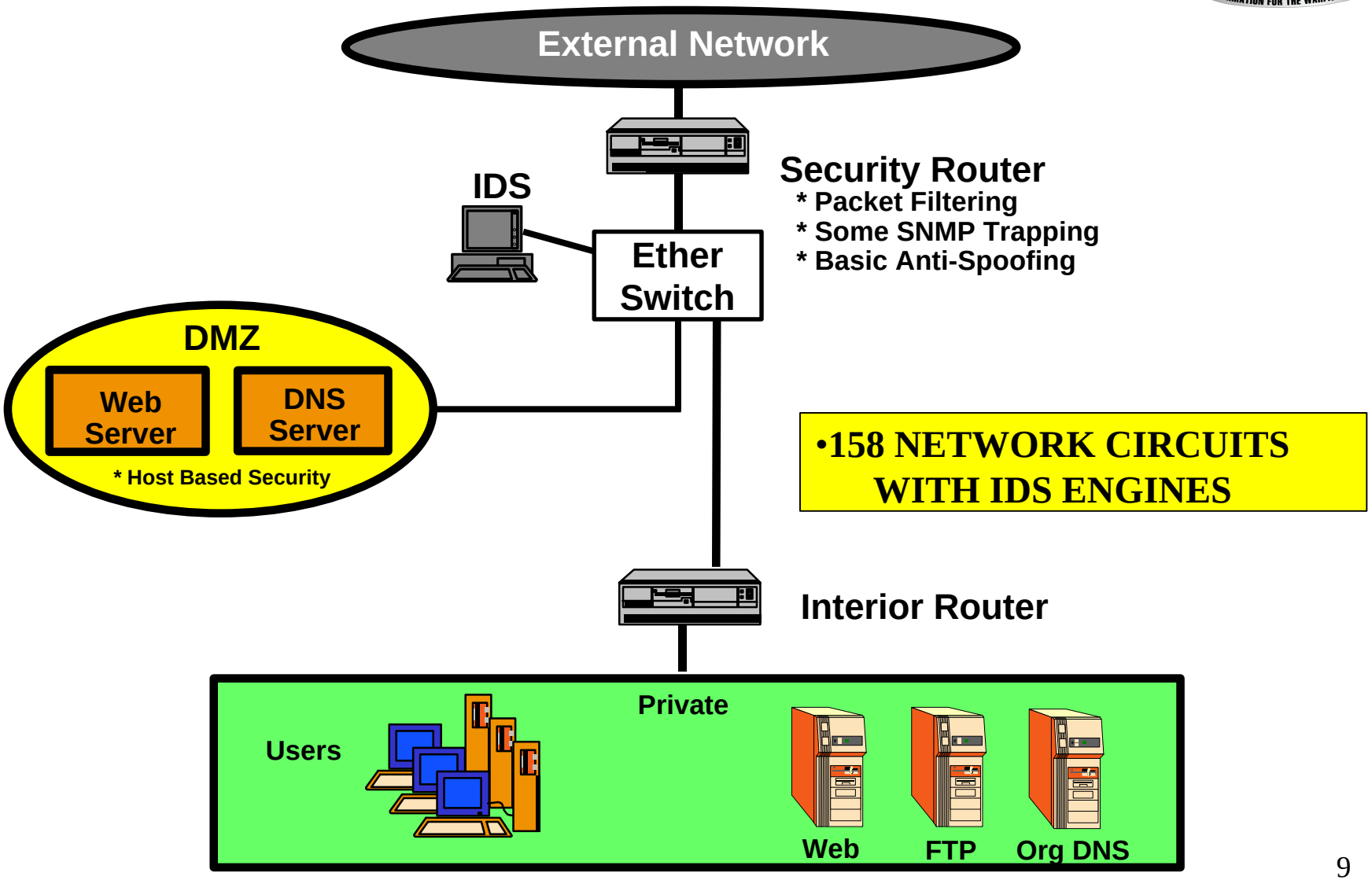
DATA IS CURRENT TO WITHIN 5-15 MINUTES



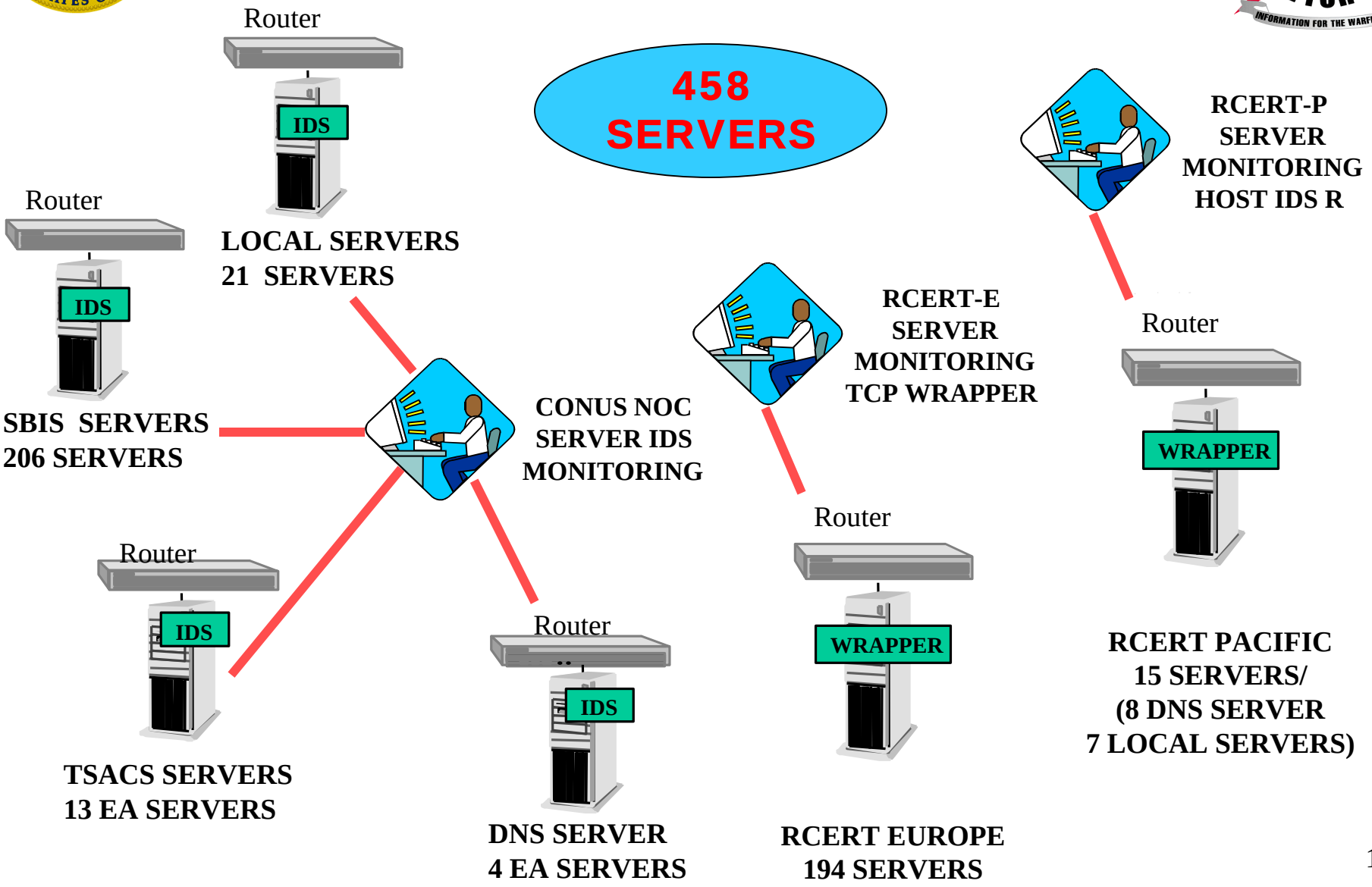
Monitoring network router status on a 24 X 7 response

Monitors US Army classified and unclassified network routers

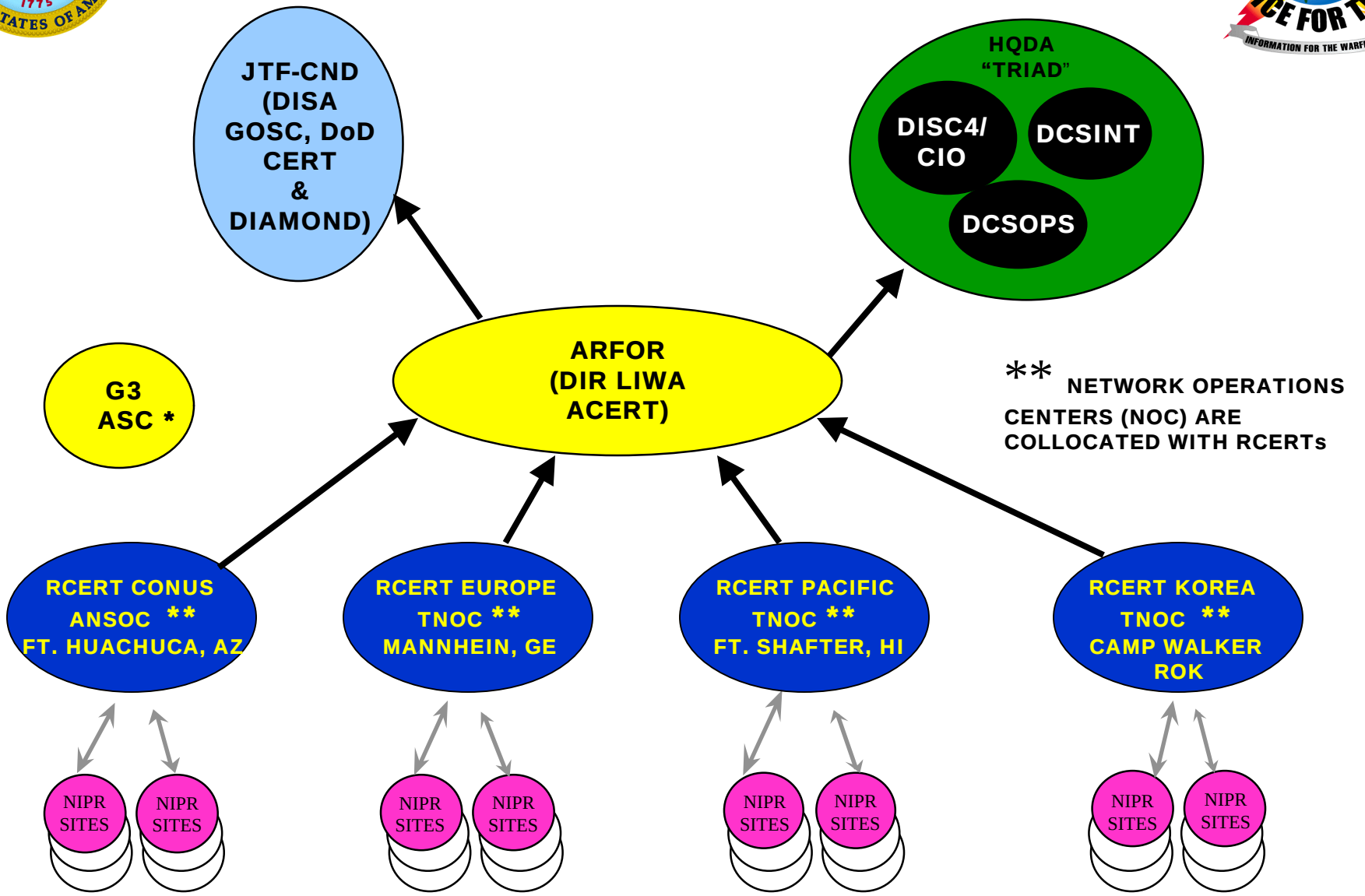
IDS SECURITY ARCHITECTURE



CRITICAL SERVERS



ACERT INFRASTRUCTURE



* RCERT OPERATIONS/ACTIONS/REPORTING COORDINATED AND INTEGRATED WITH NOC OPERATIONS

Information Assurance Vulnerability Alert

PEO/PM IAVA RESPONSIBILITIES

FIELDED SYSTEM REQUIREMENTS:

- SYSTEMS MUST MEET STANDARDS DIRECTED VIA ARMY IAVA MESSAGES
- CONFIGURATION BASELINE MANAGEMENT RESPONSIBILITY MUST BE CLEAR
- MUST BE ABLE TO INCORPORATE SECURITY PATCHES DURING LIFE CYCLE
- WHO MAINTAINS BASELINE AND HOW ARE CHANGES VALIDATED, DISSEMINATED AND INSTALLED ?

SYSTEMS IN DEVELOPMENT REQUIREMENTS:

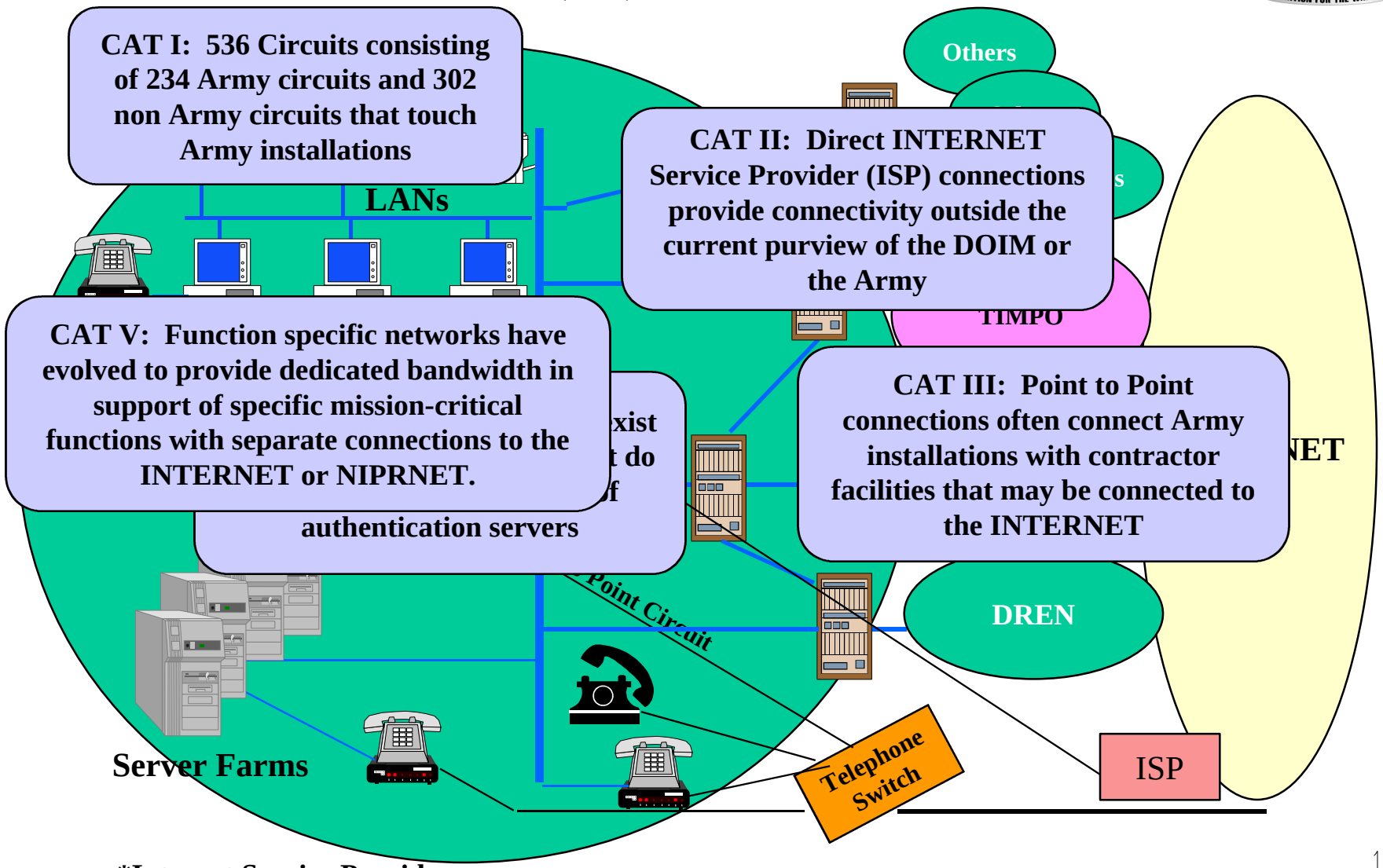
- ENSURE DISSEMINATION OF IAVA REQUIREMENTS TO DEVELOPERS
- DO NOT FIELD IF SYSTEM IS NOT IAW NSIP STANDARDS


Network Security Improvement Program
NSIP


Network Security Improvement Program
NSIP

BACK DOOR SITUATION

(Part I)



*Internet Service Provider

BACK DOOR SITUATION

CAT I: Circuits that touch Army installations - more non-Army circuits than Army circuits

CAT II: Direct INTERNET Service Provider (ISP) connections provide connectivity outside the current purview of the DOIM or the Army

CAT III: Point to Point connections often connect Army installations with contractor facilities that may be connected to the INTERNET

CAT IV: Dial-up capabilities exist throughout the installation that do not use the enhanced I&A of authentication servers

CAT V: Function specific networks have evolved to provide dedicated bandwidth in support of specific mission-critical functions with separate connections to the INTERNET or NIPRNET.

CIRCUITS IMPACTING ARMY

- THERE ARE 110 ARMY PURCHASED CIRCUITS IN CONUS -- 108 CIRCUITS ARE PROTECTED WITH ARMY NSIP IDS SECURITY PACKAGE -- 98 %
- THERE ARE 58 ARMY PURCHASED CIRCUITS OCONUS -- 55 CIRCUITS ARE PROTECTED -- 95 %
- THERE ARE 136 NON ARMY CIRCUITS THAT CONNECT TO AN ARMY INSTALLATION IN CONUS
- THERE ARE 166 NON ARMY CIRCUITS THAT CONNECT TO AN ARMY OCONUS INSTALLATION
- THERE ARE ISP CONNECTIONS AND POINT TO POINT CONNECTIONS THAT ARE BEING RESEARCHED/IDENTIFIED


Network Security Improvement Program
NSIP

AUTHENTICATION OF LOGIN AND PASSWORD

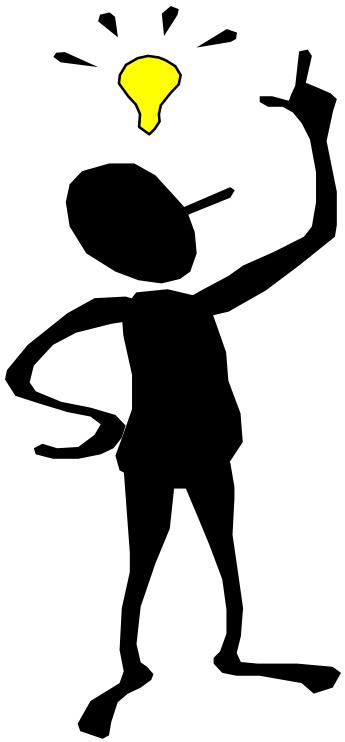
- **NETWORK SECURITY IMPROVEMENT PROGRAM (NSIP) -- ARMY MODEM DIAL-IN STANDARDS AND POLICY --*DTG 231300Z APRIL 99***

- **MAIN POINTS:**
  - **-- migrate to an identification and authentication system that authenticates all dial-in operations with a unique user ID and password**
  - **-- JTA compliant with the Remote Authentication Dial-in User System (RADIUS)**
  - **-- RADIUS software configured for logging**
  - **-- authentication server monitored with a host based IDS**
  - **-- report type/location of authentication servers**
  - **-- remote configuration audit of authentication server**
  - **-- configuration of dial-in systems**

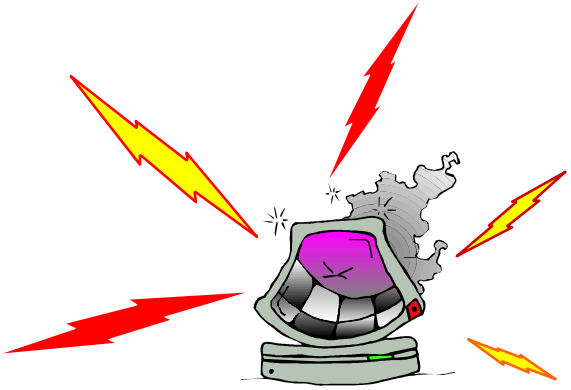
- **ARMY organizations not having an authentication server capability MAY coordinate for use of the TSACS authentication servers**


Network Security Improvement Program
NSIP

BIOMETRIC TECHNOLOGY

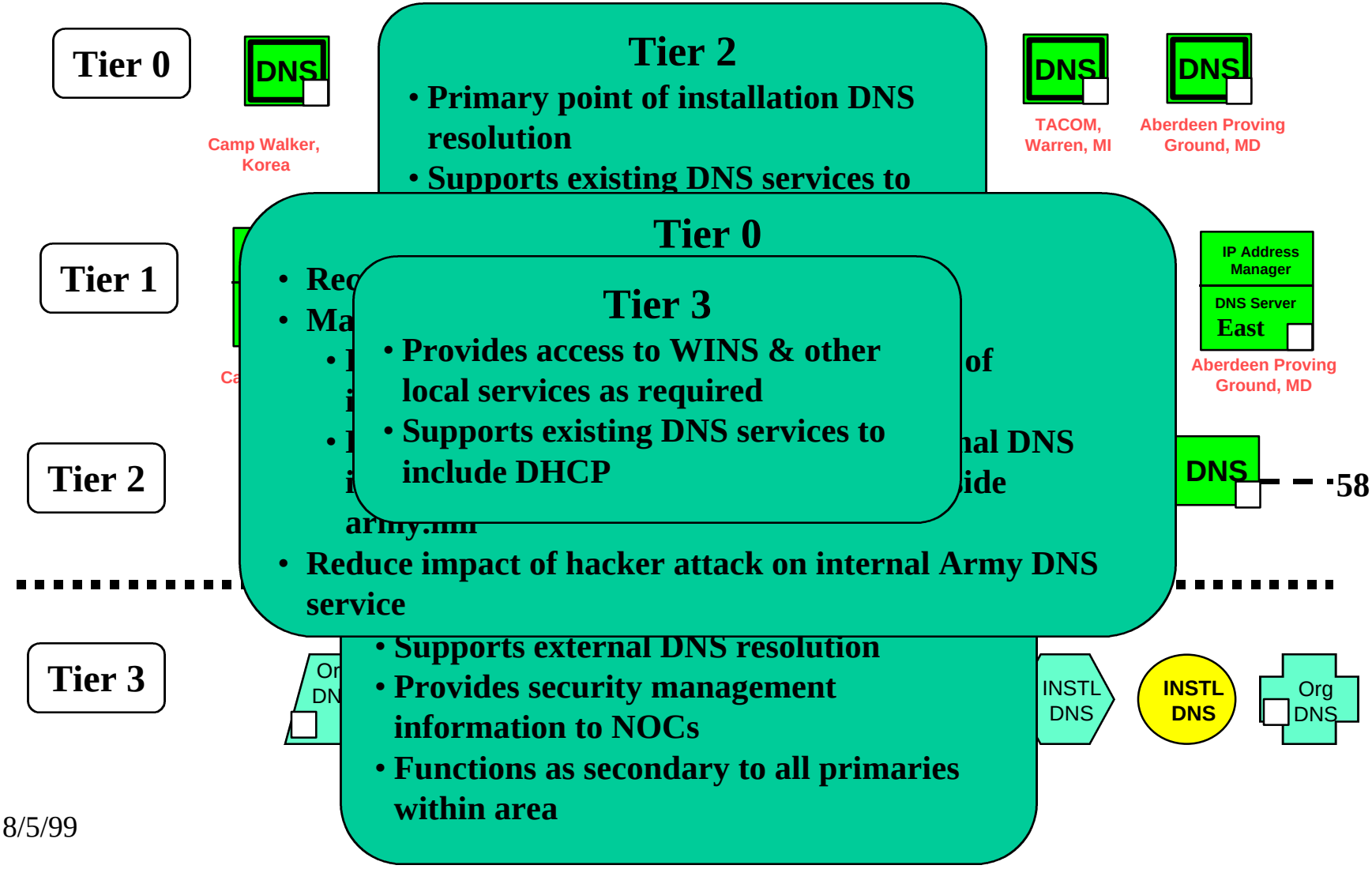


- FINGERPRINT RECOGNITION
- VOICE RECOGNITION
- IRIS

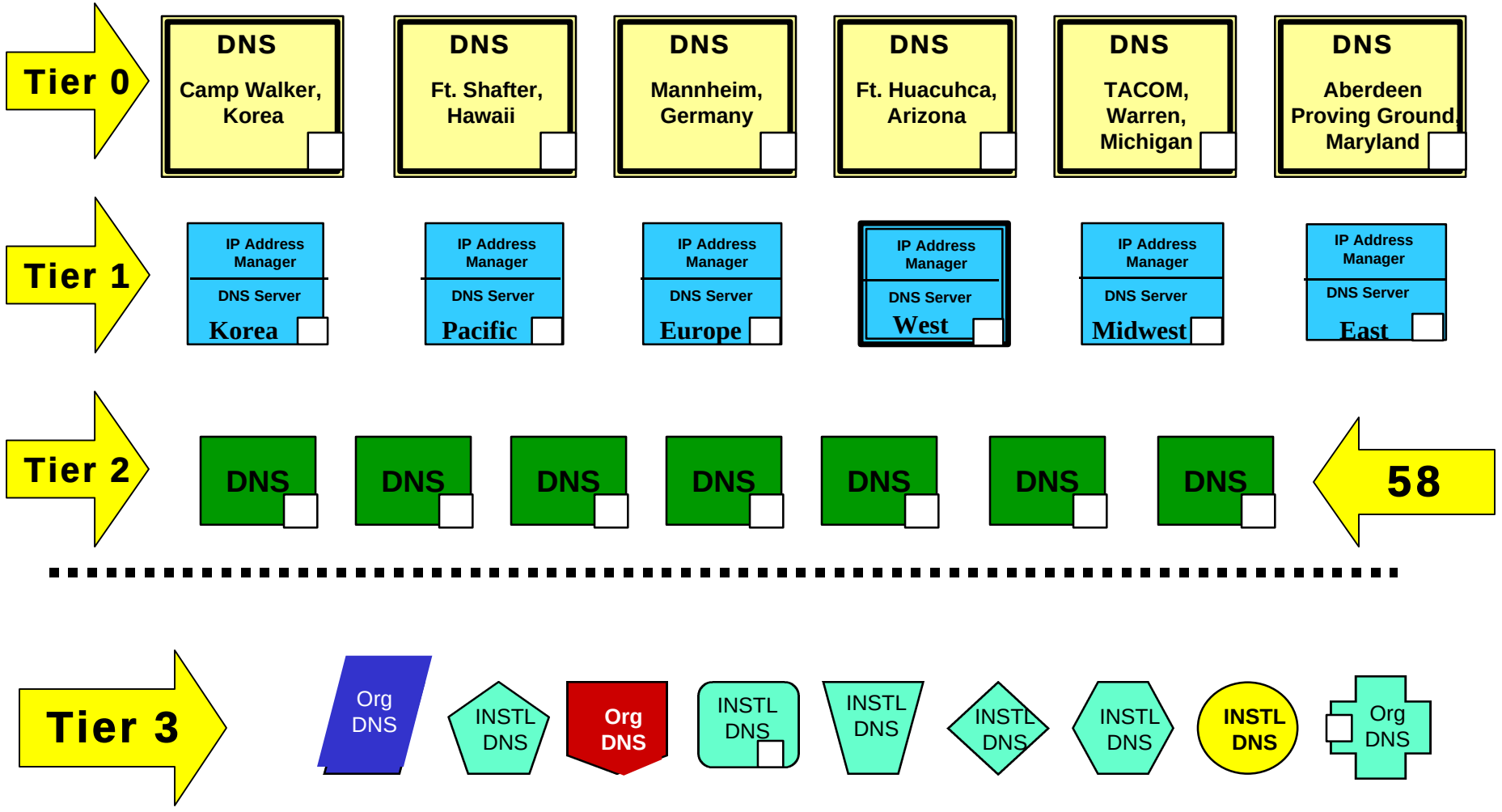



Network Security Improvement Program
NSIP

DNS DESIGN TOPOLOGY



PROTECTED DNS



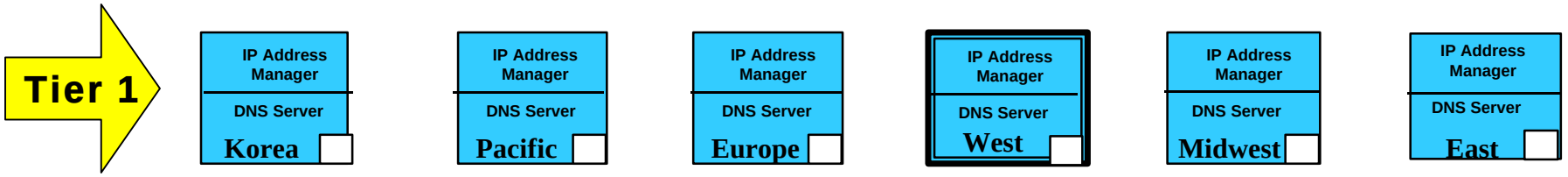
PROTECTED DNS -- TIER 0

Tier 0

- **Receives/Responds to external queries**
- **Maintain anonymity of Army DNS system**
  - **Rewrite of name server record that indicates source of information**
  - **Rewrite of server records to prevent additional DNS information from being accessed**

2800
Data Dump
Requests
Denied -
Foreign and
Domestic

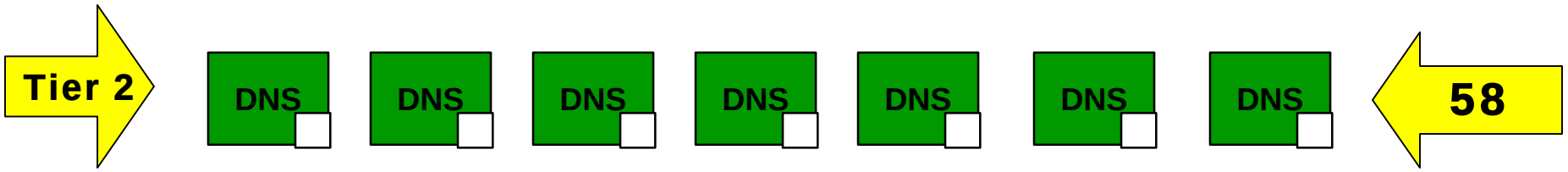
PROTECTED DNS -- TIER 1



Tier 1

- IP Manager and DNS server integrated into 1 box
- Each tier 1 server contains all Army DNS information
- Resolves external DNS resolution for tier 0
- Functions as secondary to all tier 2 DNS servers within geographic area for internal queries
- Provides security management information to Network Operation Centers (NOC)

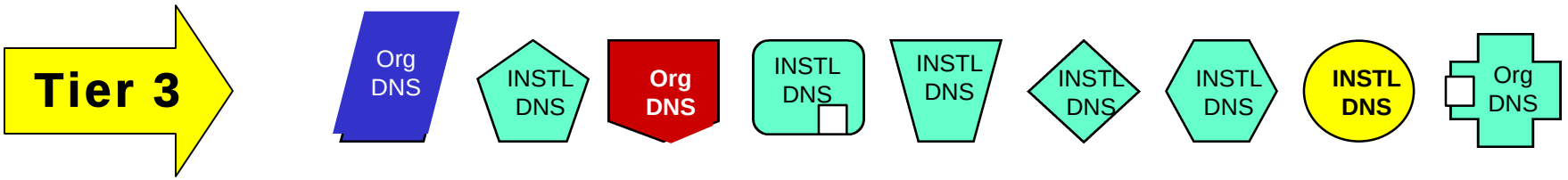
PROTECTED DNS -- TIER 2



Tier 2

- **Primary point of installation DNS resolution**
- **Supports existing DNS services to include DHCP**

PROTECTED DNS -- TIER 3



Tier 3

- **Provides access to WINS & other local services as required**
- **Required to meet configuration standards**


Network Security Improvement Program
NSIP

FIREWALL POLICY

- **Firewall Message -- DTG 301200Z APRIL 99**
  - ITEMS DISSCUSED:

    ---Authorized firewall products
    --- Least privileged
    --- Coordination with supporting theater NOC and RCERT
    --- Perimeter/border versus critical server/enclave

  - ADDITIONAL DISCUSSION:

    ---Architecture
    ---Implementation
    ---Configuration
    ---Testing


Network Security Improvement Program
NSIP

SIPRNET
CONCEPT OF OPERATION

- ***Map*** the SIPRNet on an installation
- ***Use*** scanner to discover network hosts and vulnerabilities
- ***Research*** existing policies and procedures
- ***Evaluate*** SIPRNet DNS solution
- ***Evaluate*** tactical interface

- ***Develop*** Army standard policies, procedures and hardware/software solutions.
- ***Implement*** Army standard policies, procedures and hardware/software solutions FY 2000.

SIPRNET INITIATIVE

- The Theater Signal Command owns and operates the Army SIPRNet backbone in Europe and will conduct a pilot NSIP SIPRNet initiative:

- Apply Router Packet Filtering/Access Control Lists to SDN-SIPRNET perimeter routers -- August 99.

- Install and monitor 4 network IDS and 10 host based IDS -- September 99.

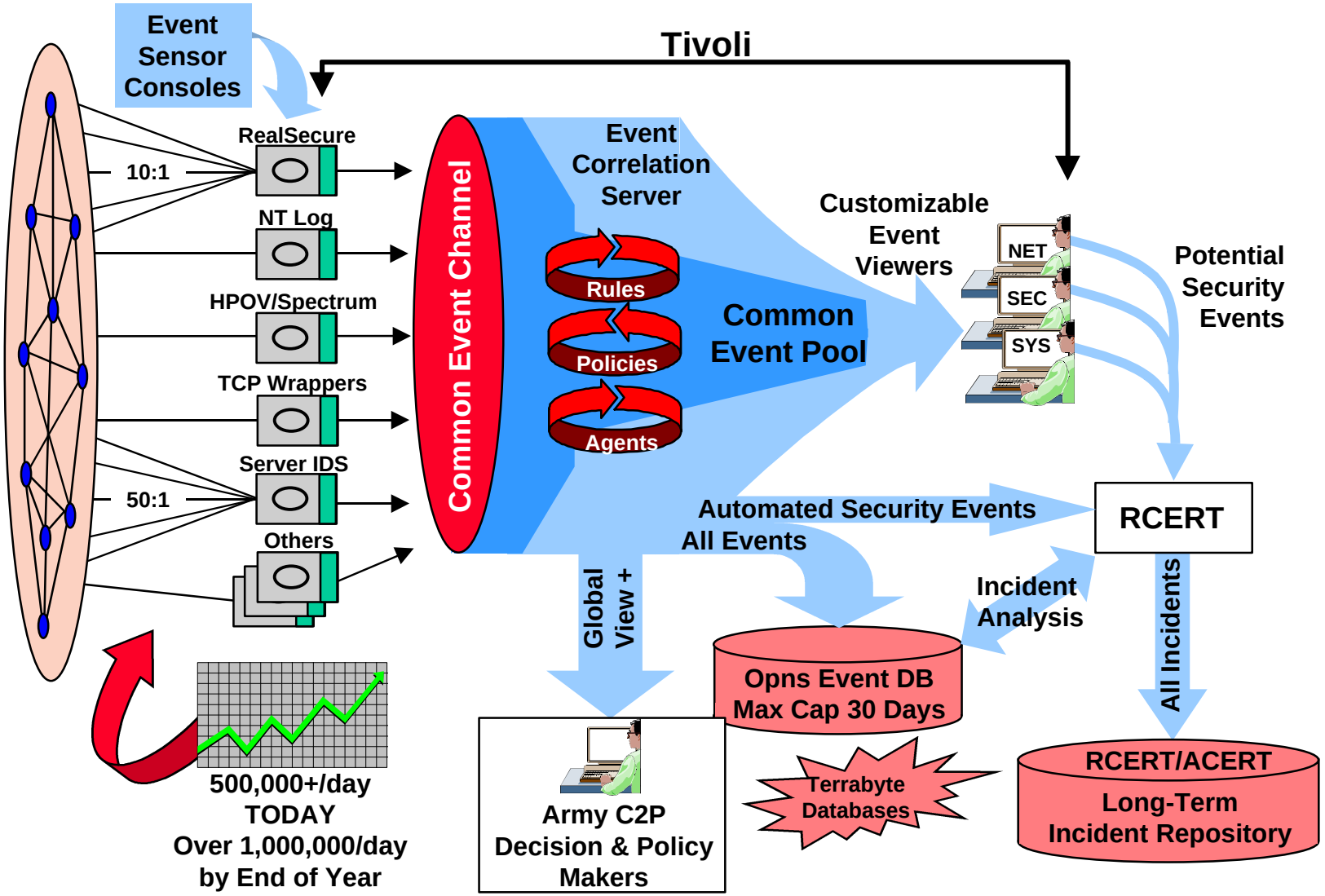
- Complete host based IDS fielding (estimated 80 servers) and expand ACLs to customer routers -- December 99.

- Implement Authentication Servers for dial-in and field remainder of network IDS (approximately 25) -- March 00.

- FOC for security-in-depth solution for the Army SIPRNet in Europe -- September 00.


Network Security Improvement Program
NSIP

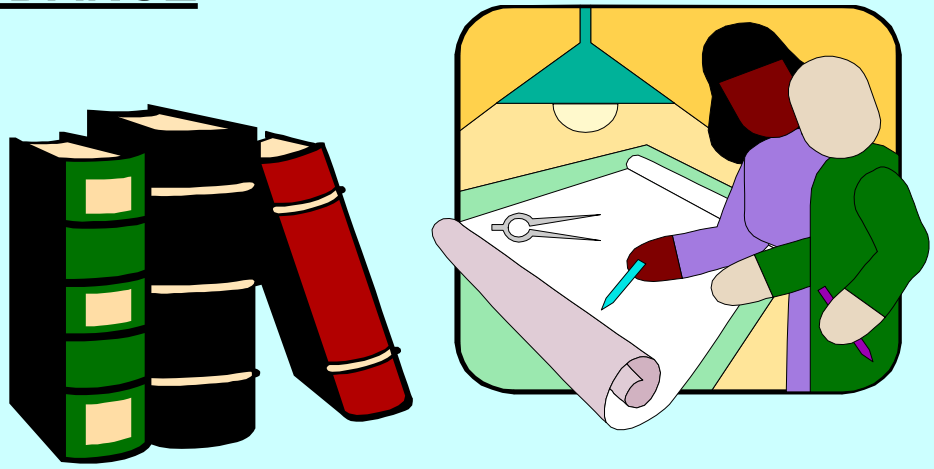
INFORMATION ASSURANCE SENSOR CORRELATION




Network Security Improvement Program
NSIP

INSTALLATION INFORMATION INFRASTRUCTURE ARCHITECTURE (I3A)

GUIDANCE



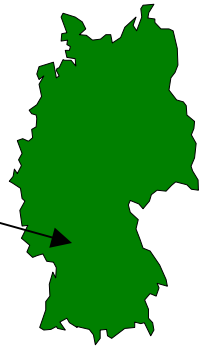
ARCHITECTURE


Network Security Improvement Program
NSIP

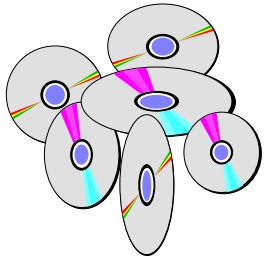
TRAINING

NOTE: Figures are approximate numbers of personnel trained annually

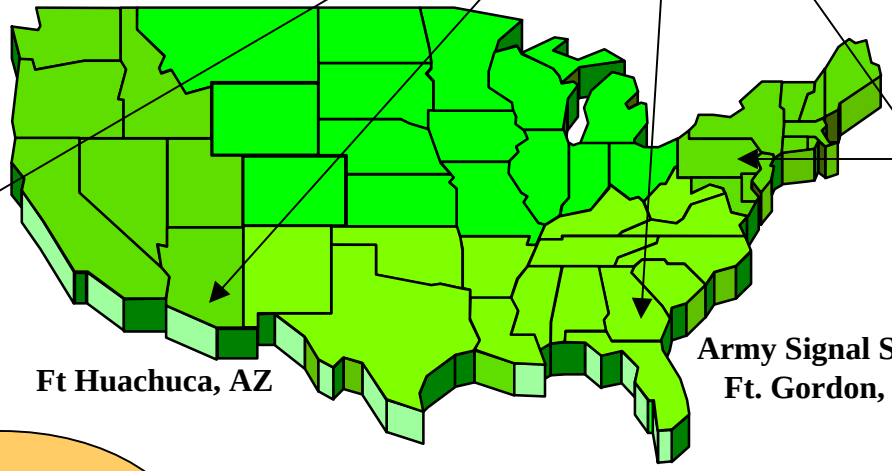
Resident/ "School House" Instruction
Military, DA Civilians & Contractors
System Administrators/Network Managers: 800
Technical IDS & Firewall Training: 300



Mannheim, GE



800 + Computer Based Training Courses



Congressionally Sponsored University IA Programs

Ft Shafter, HI

Ft Huachuca, AZ

Army Signal School Ft. Gordon, GA

Taegu, S. Korea

IA Officer Mobile Training Teams World-wide 600

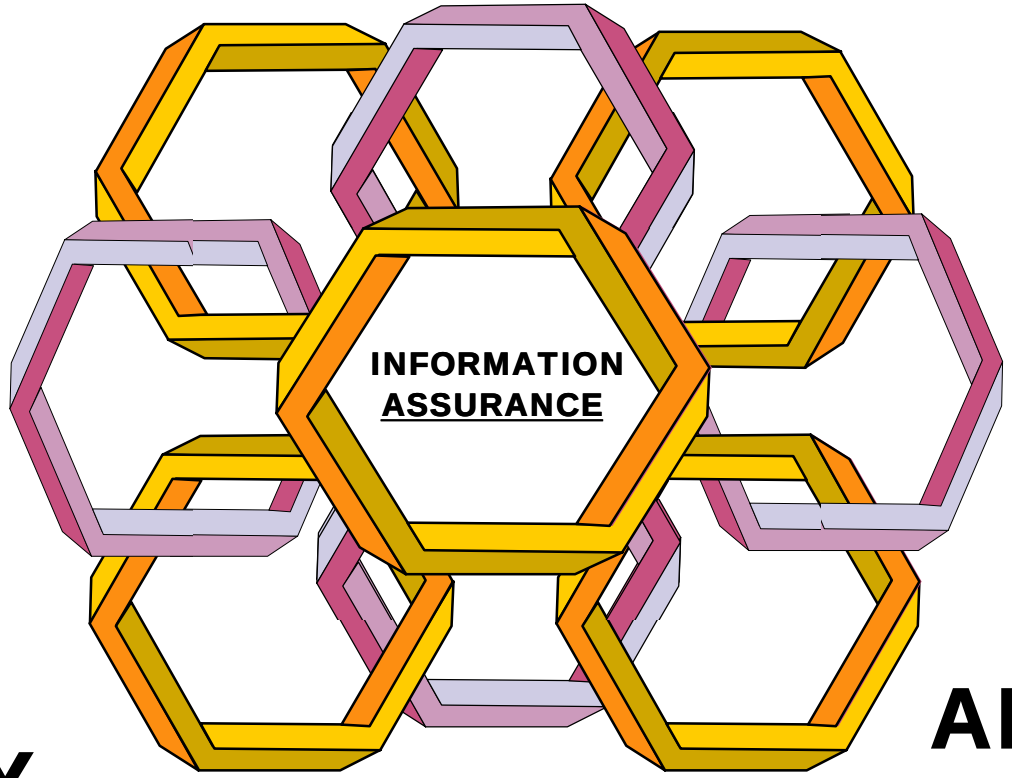
Quarterly Workshops World-Wide 800

Retention Study Underway


Network Security Improvement Program
NSIP

POLICY

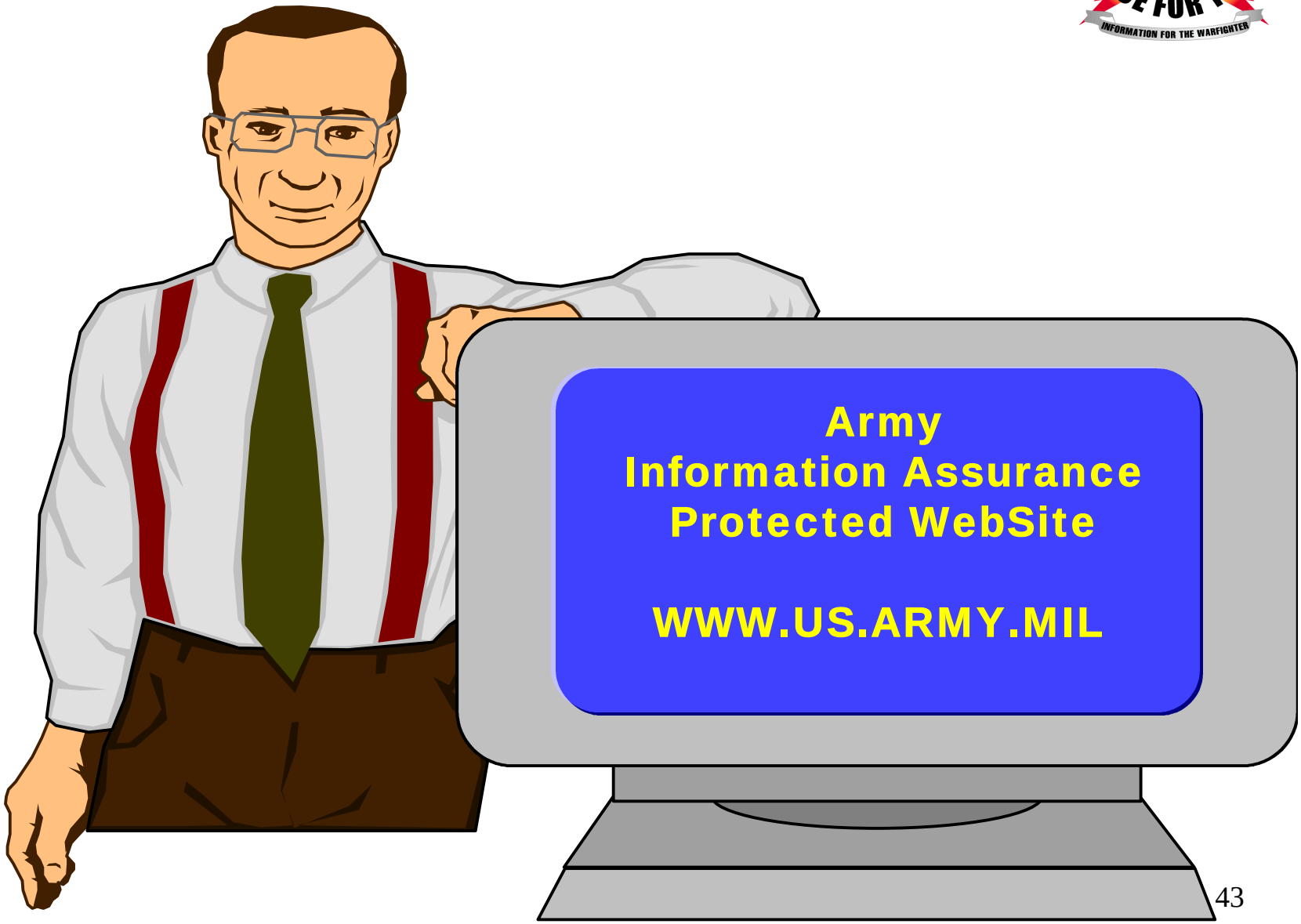
AR 25 - 1



ARMY PAM 25 - IA

ARMY REGULATION 25 -IA

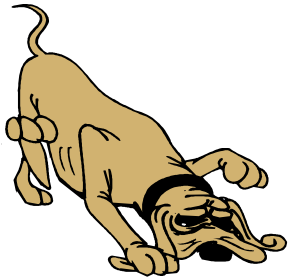
INFORMATION INITIATIVE



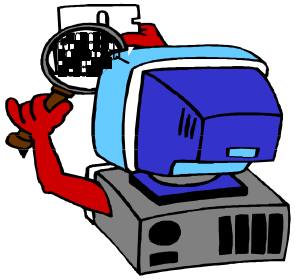

Network Security Improvement Program
NSIP

C2 PROTECT TOOLS

- **TYPES OF TOOLS**
  - **-- ToneLoc -Wardialer**
  - **-- OPIE- 8 character password generator**
  - **-- E-TKNED -mapping/scanning tool**
  - **-- E-SATAN -scanning tool**
  - **-- Sentinel Detection Tool Kit (ARL developed IDS type scripts)**
  - **-- TCP/IP Wrappers**
  - **-- SPI TOOLS**



- **COTS PRODUCTS**
  - **-- Real Secure**
  - **-- ISS Scanner**
  - **-- AXENT**
  - **-- Anti-Virus (DoD licensed: Norton & McAfee)**



- **NEW TOOLS**
  - **-- Army license for network/host IDS and firewall**
  - **-- Modified “cracker” tool for UNIX and NT**


Network Security Improvement Program
NSIP

DoD DRAFT PKI POLICY HIGHLIGHTS

- All DoD components will deploy an infrastructure with the capability to issue Class 3 digital certificates by October 2000
- All DoD users will be issued a Class 3 certificate by October 2001
- All e-mail (as distinct from organizational messaging) will be digitally signed beginning October 2001
- DoD will replace Class 3 certificates with Class 4 certificates beginning June 2002

DoD DRAFT PKI POLICY HIGHLIGHTS

- **All private (non-public accessible) WEB servers containing DoD information will use Class 3 Certificate for server authentication and use Secure Sockets Layer (SSL) by June 2002**

- **All WEB clients will require a Class 3 certificate for I&A to above servers by October 2001**

DoD DRAFT PKI POLICY HIGHLIGHTS

- **Two primary PKI efforts**
  - FORTEZZA-based PKI (near term solution for Class 4)
  - Class 3 (formerly Medium Assurance) PKI

Class	*User Identification*	*User Token*	*Algorithms*
4 (High)	In person	Hardware (Smart card/FORTEZZA)	Type II
3 (Medium)	In person	Software	Type II

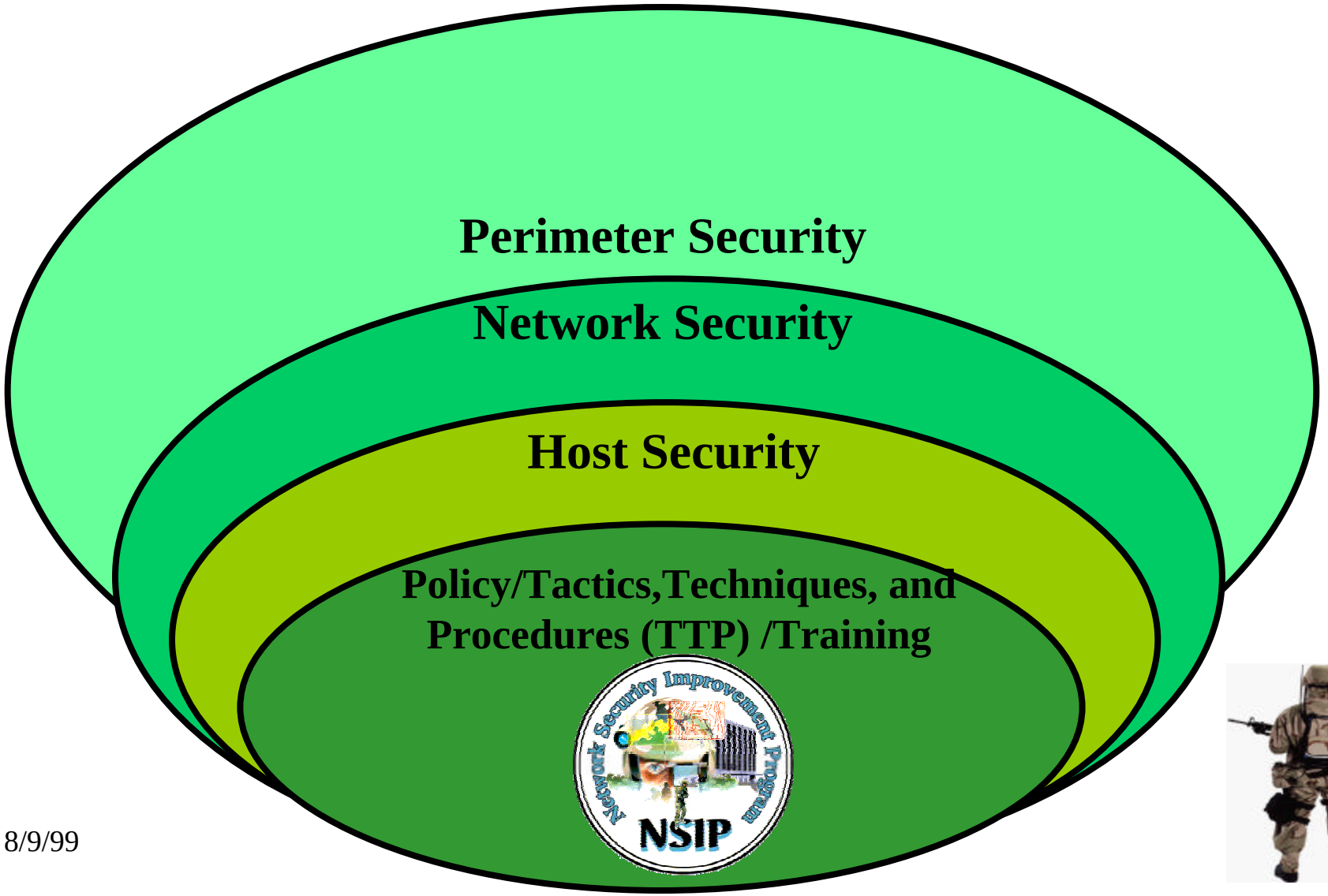
- **DoD will issue two types of certificates**
  - Identify - for identification & authentication (I&A) and digital signature
  - Encryption (e-mail) - for encryption only

ARMY PKI POLICY HIGHLIGHTS

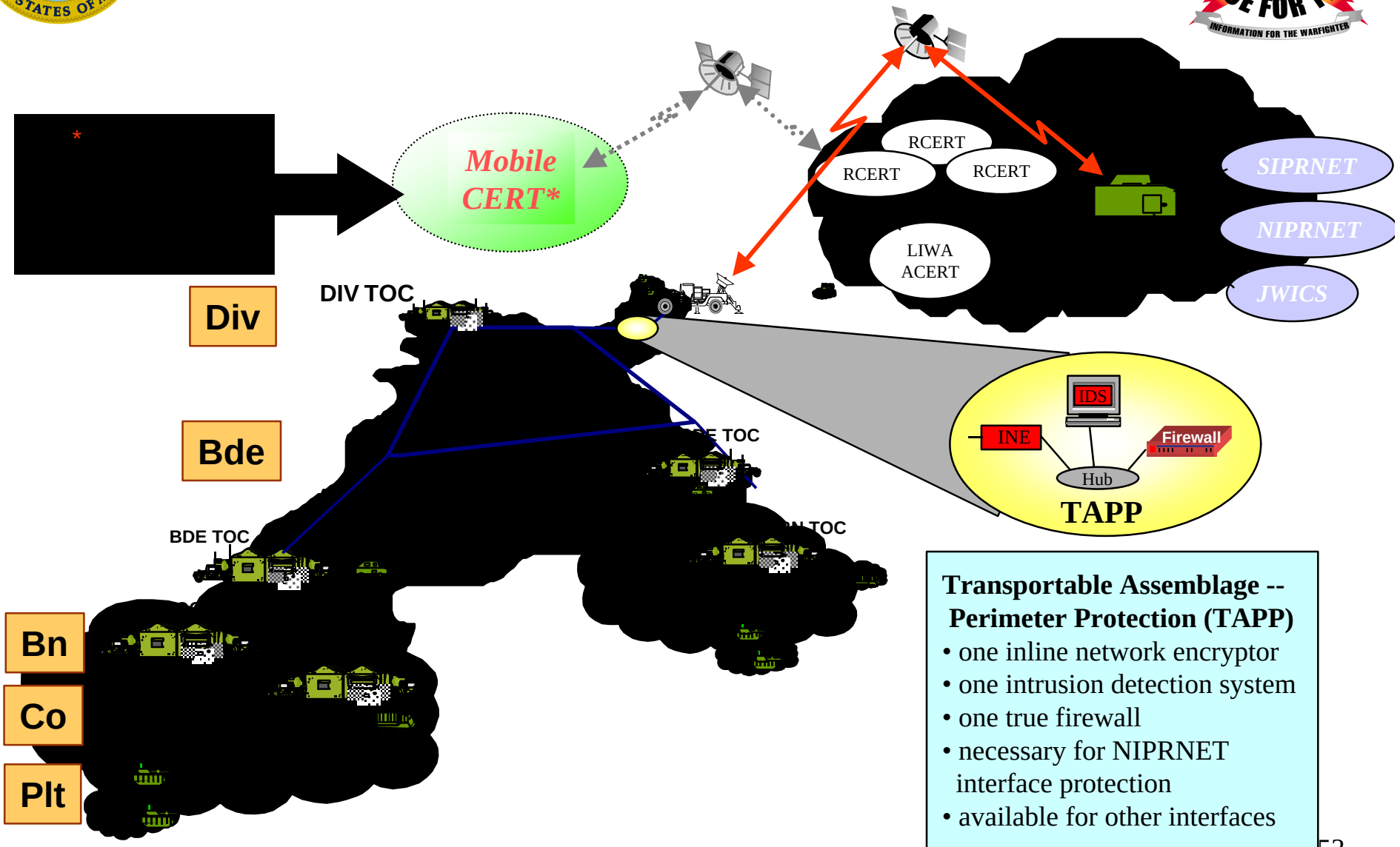
- Army will comply with DoD PKI policy
- Army will use DoD PKIs only


Network Security Improvement Program
NSIP

SECURITY IN DEPTH FOR THE FDD



EXTERNAL INTERFACE (REACHBACK) NETWORK SECURITY MECHANISMS



Transportable Assemblage -- Perimeter Protection (TAPP)

- one inline network encryptor
- one intrusion detection system
- one true firewall
- necessary for NIPRNET interface protection
- available for other interfaces

TACTICAL INITIATIVE

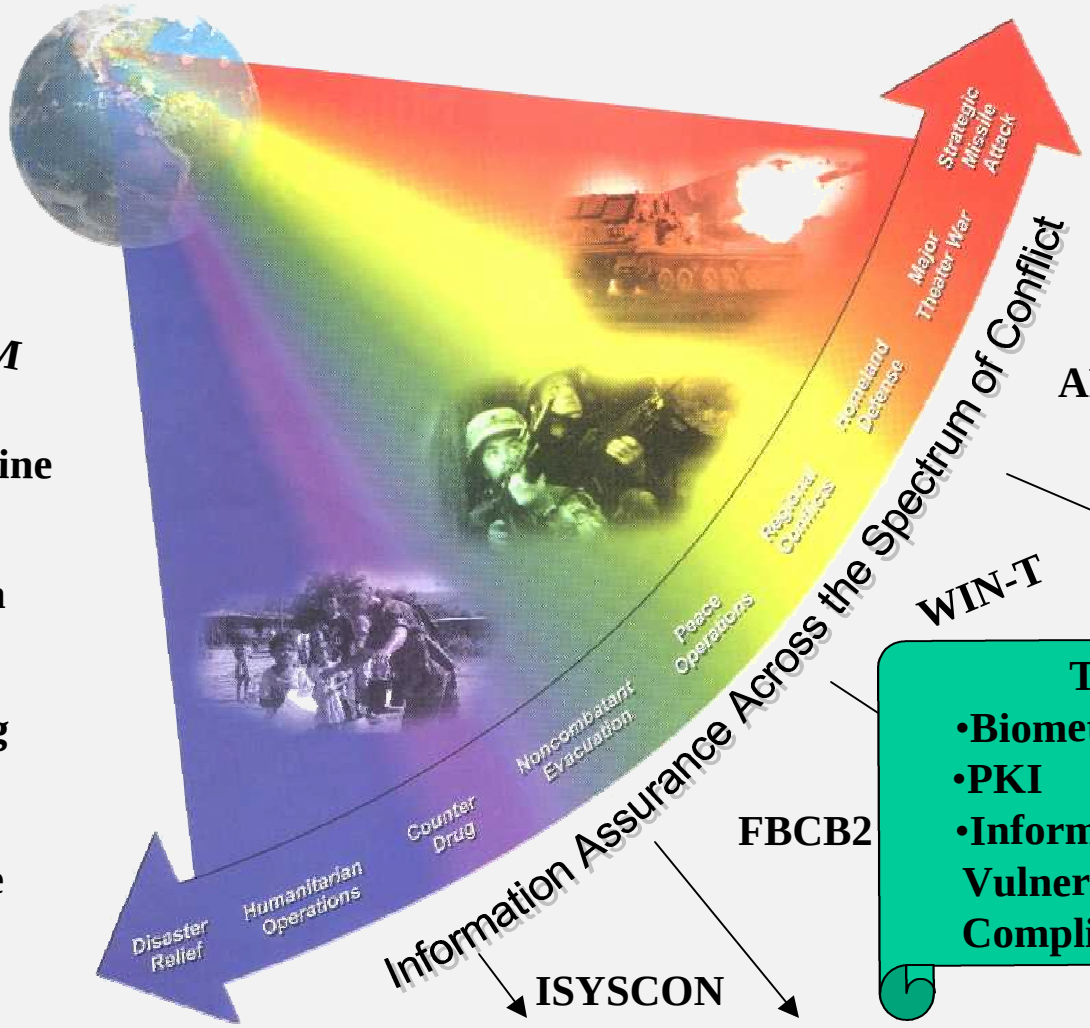
- **RCERT-EUROPE will validate the use of and integrate Tactical Assemblage Perimeter Packages (TAPP) into unit training and in support of real-world deployments.**

- **Test and implement with 7th Signal Brigade -- Theater Tactical Signal Brigade -- December 99.**

- **Test and implement with 7th Signal Brigade -- Corps Signal Brigade -- December 99.**

- **Prepared to deploy in support of real-world deployments -- June 00.**

CONCLUSION



Distance Learning

Y2K

ATM

Telemedicine

Power Projection

Sustaining Base

E-Commerce

GCCS-A

AFATDS

ABCS

FDD

WIN-T

FAADC2I

FBCB2

ISYSCON

The Future

- **Biometrics**
- **PKI**
- **Information Assurance Vulnerability Alert (IAVA) Compliance Verification**

FULL DIMENSIONAL PROTECTION