



# IT Governance CEB

VADM Dennis McGinn

Deputy, Chief of Naval Operations (Warfare  
Requirements and Programs) &  
Navy Information Officer

703-693-7660

McGinn.Dennis@hq.navy.mil



# Agenda

- Scope of IT
- Progress to Date
- CNO CEB Questions
- The Challenges
- Navy Information Officer Actions
- What's Next



# Scope of IT

## Information Technology (IT).

Any equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information ..... includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related services.

Source: Clinger-Cohen Act of 1996

The term “IT” also includes **National Security Systems (NSSs)**

- intelligence activities;
- cryptologic activities related to national security;
- command and control of military forces;
- equipment that is an integral part of a weapon or weapon system or
- equipment critical to the direct fulfillment of military or intelligence missions

Source: Section 5142, Title 40 U.S. Code 1401 &  
Executive Order 13011 dtd 17 JUL 1996



# Progress to Date

- IT21 and NMCI
- Task Force Web
- Navy Applications Database Task Force (NADTF)
- Functional Area Managers (FAM)
- Enterprise Application & Database Management Processes
- NetWarCOM
- FORCEnet



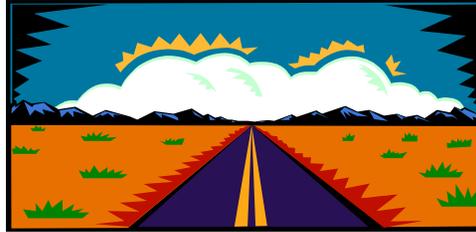
# CNO CEB Questions

## Questions/Issues from previous CEBs

- What does the master architecture look like and how will Navy manage IT that is outside NMCI architecture? Include in the answer the potential for operating a network(s) outside the bounds of NMCI as well as benefits and risks.
- Explain how everyone in the Navy can get internet access and the costs of that access Including account for life, digital ID and SELRES Seats.
- What is the potential for operating a network(s) or architecture outside the bounds of NMCI as well as benefits and risks?
- What is the overall architecture between IT21/NMCI/BLII/FORCEnet?
- What is the potential impact of critical systems that are not compliant with either NMCI or TASK FORCE WEB standards?
- How both legacy and new applications and systems are to be assessed, migrated, or acquired in compliance with the transition plans for both NMCI & TASK FORCE WEB?
- Will we achieve the directed 95% reduction of legacy applications within one year?
- What is the estimated costs associated with migrating systems into compliance with NMCI as well as for TASK FORCE WEB?
- How does the Risk Mitigation Process work with respect to quarantined Applications?



# IT: Local NOT Corporate



## IT21 & NMCI a Corporate Road Ahead .....

**LITTLE CORPORATE  
RESOURCE VISIBILITY**

**DISCONNECTED  
INTEGRATION**

**ENFORCEMENT  
MECHANISM UNDEFINED**

**INFORMATION  
ASSURANCE ABYSS**

**DISPARATE  
DATABASES**

**LEGACY APPS**

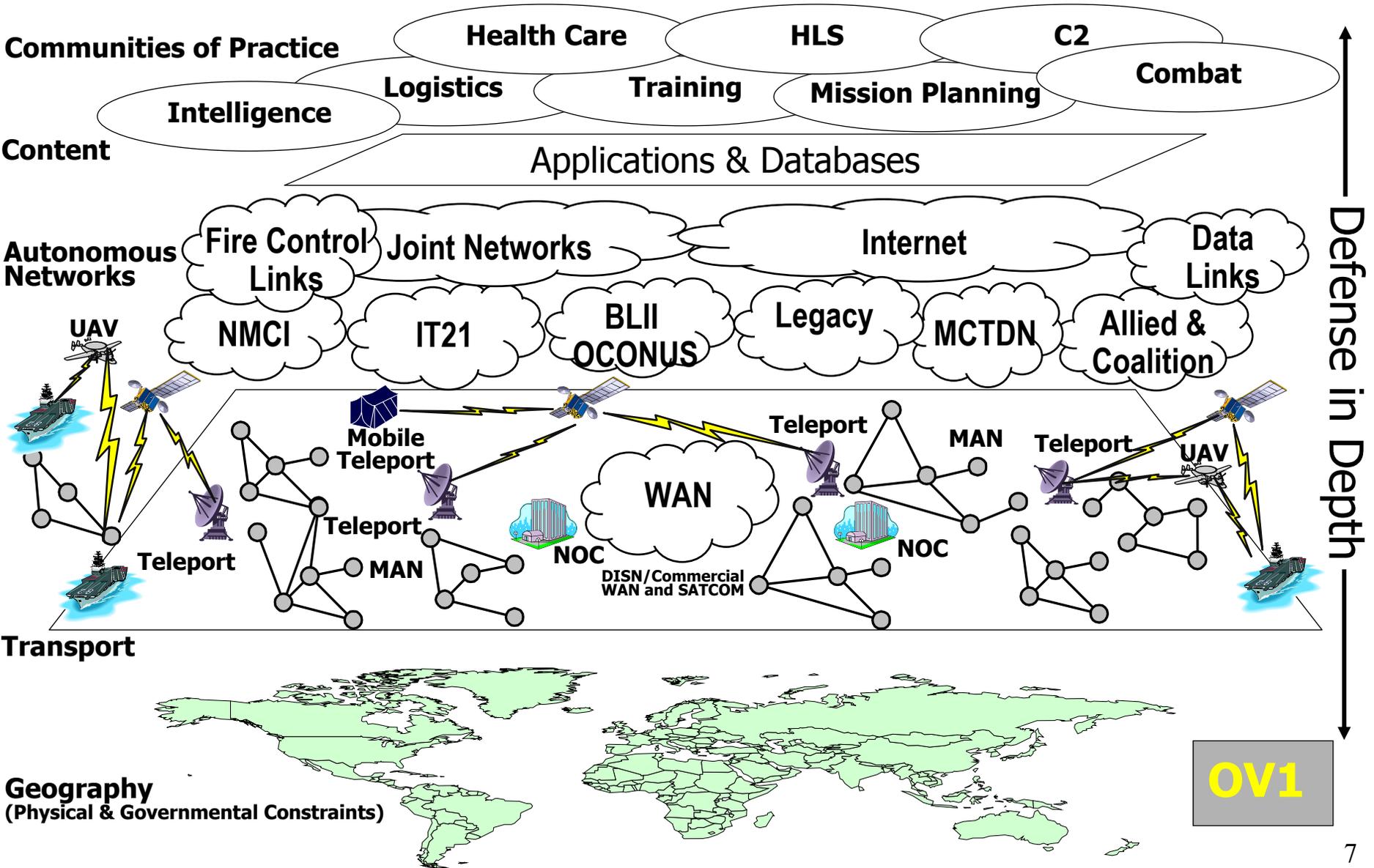
**ROGUE NETWORKS**



**...and found major potholes**



# Today's Architecture









# Definitions .....

## Governance

The act, process or power of controlling actions and behavior.

### **Authority for**

- Policy and Oversight
- Requirements
- Resources/Funding
- Acquisition
- Operations/Enforcement



# Way Ahead

- NIO establish and enforce Navy IT Policies
- Identify IT Corporate Governance Structure
- Designate IT Architect & Technical Authority
- Achieve Visibility into & Control of IT Resources and Funding throughout Navy
- Determine Total Navy IT Requirements
- Focus on Security & Risk Mitigation
- Identify IT Options with NMCI Contract
- Answer CNO Questions

**Corporate IT Governance a key to FORCEnet implementation !**



# BACKUPS



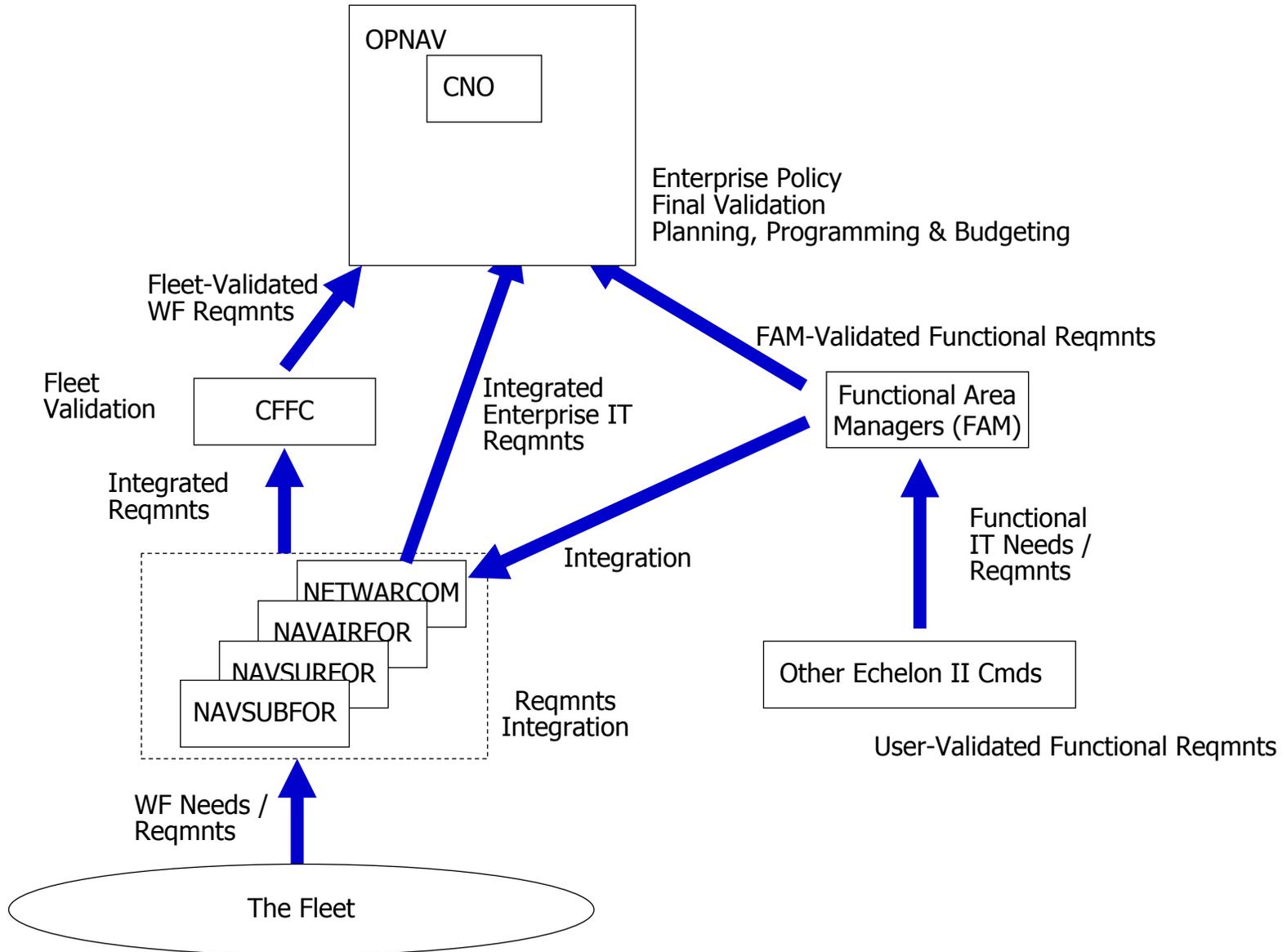
# CNO CEB Questions

## Questions/Issues from previous CEBs

- What does the master architecture look like and how will Navy manage IT that is outside NMCI architecture? Include in the answer the potential for operating a network(s) outside the bounds of NMCI as well as benefits and risks. **Follow-on CEB**
- Explain how everyone in the Navy can get internet access and the costs of that access including account for life, digital ID and SELRES Seats. **Follow-on CEB**
- What is the potential for operating a network(s) or architecture outside the bounds of NMCI as well as benefits and risks? **Follow-on CEB**
- What is the overall architecture between IT21/NMCI/BLII/FORCEnet? **Follow-on CEB**
- What is the potential impact of critical systems that are not compliant with either NMCI or TASK FORCE WEB standards? **Follow-on CEB**
- How both legacy and new applications and systems are to be assessed, migrated, or acquired in compliance with the transition plans for both NMCI & TASK FORCE WEB? **Process**
- Will we achieve the directed 95% reduction of legacy applications within one year? **Maybe**
- What is the estimated costs associated with migrating systems into compliance with NMCI as well as for TASK FORCE WEB? **Process**
- How does the Risk Mitigation Process work with respect to quarantined Applications? **Process**



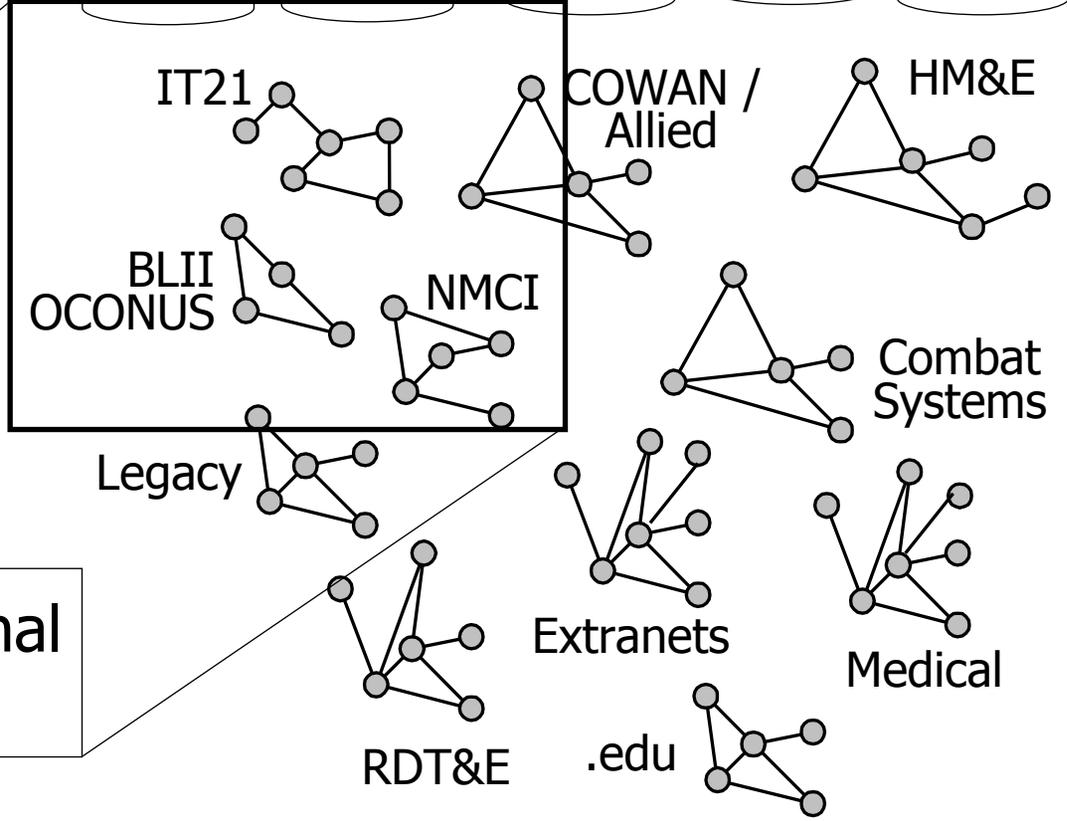
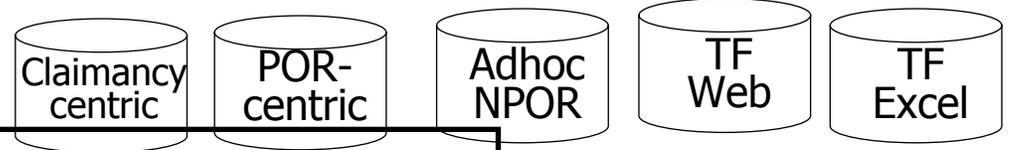
# IO / Space / IT Requirements Process





# Today's Architecture

External Factors  
 JTA  
 DISA Standards  
 USMC  
 Allied Interoperability  
 JTF Warnet  
 HLS  
 Industry Trends



NETWARCOM operational control and visibility

Apps  
 Infrastructure

*Varying levels of capability, security, interoperability*



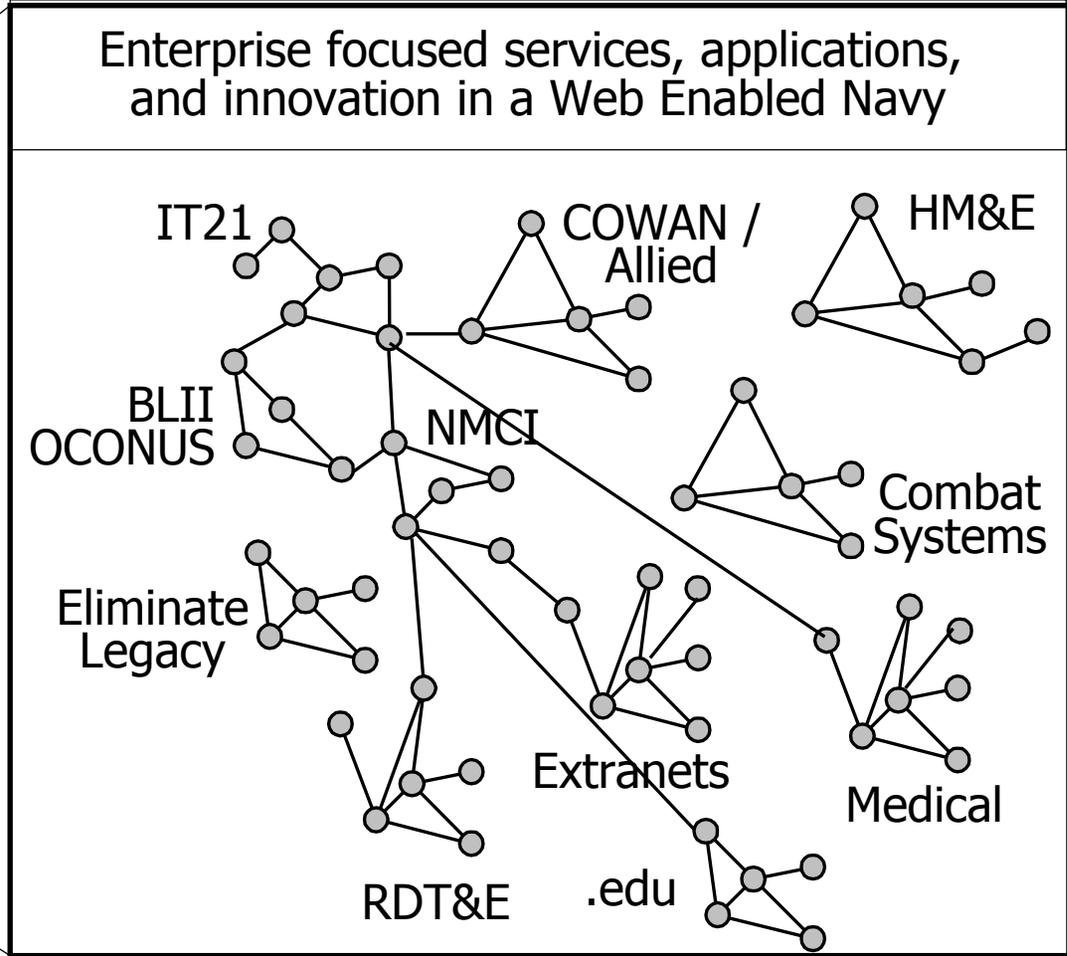
# To Be "One Naval Network"

NIO IT Policy and IT Strategy

-

NETWARCOM operational control and visibility

Common Standards, Operations & Defense in Depth



Apps

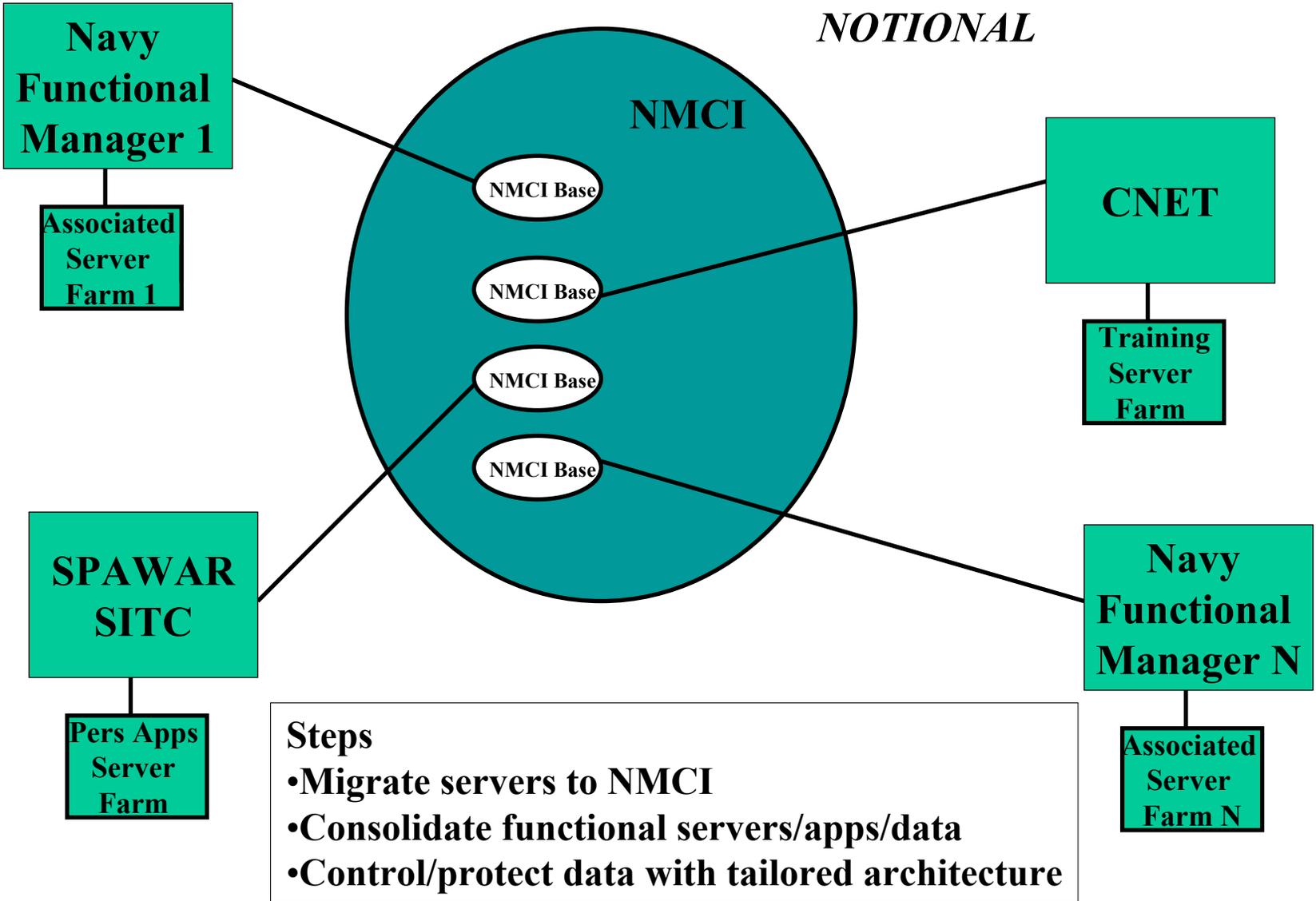
Infrastructure

**NETWARCOM enforced standards, operations, & defense**



# To-be Server Architecture Controls/ Protects Critical Corporate Data

*NOTIONAL*

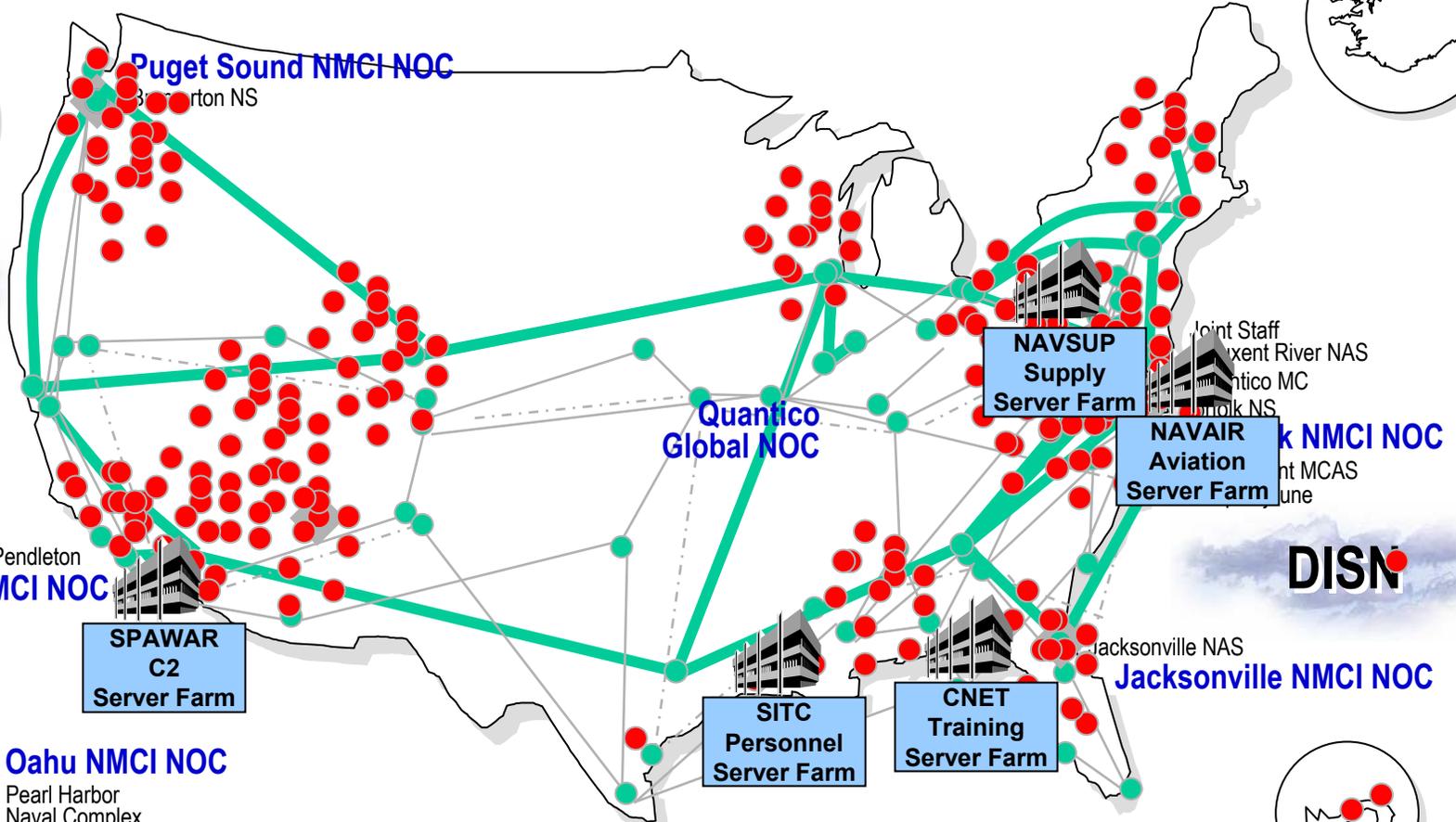




# Server Farm Consolidation



vBNS+



DISN

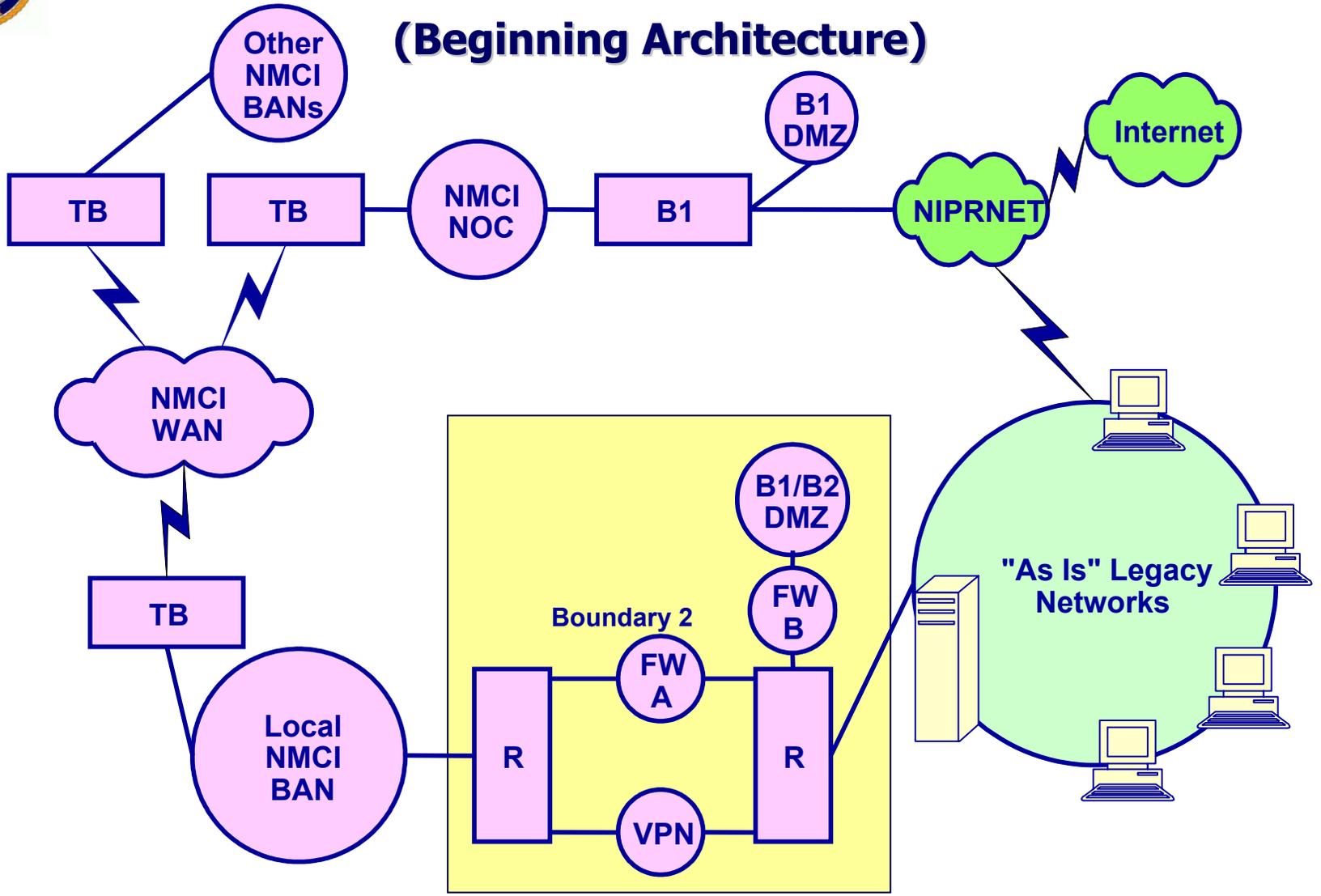
- Proliferation of data centers – increased cost
- Limited standardization
- Performance/security impacts

— OC-3 DISN DS/BMS-C  
 — OC-48 vBNS+ Backbone



# NMCI Certification

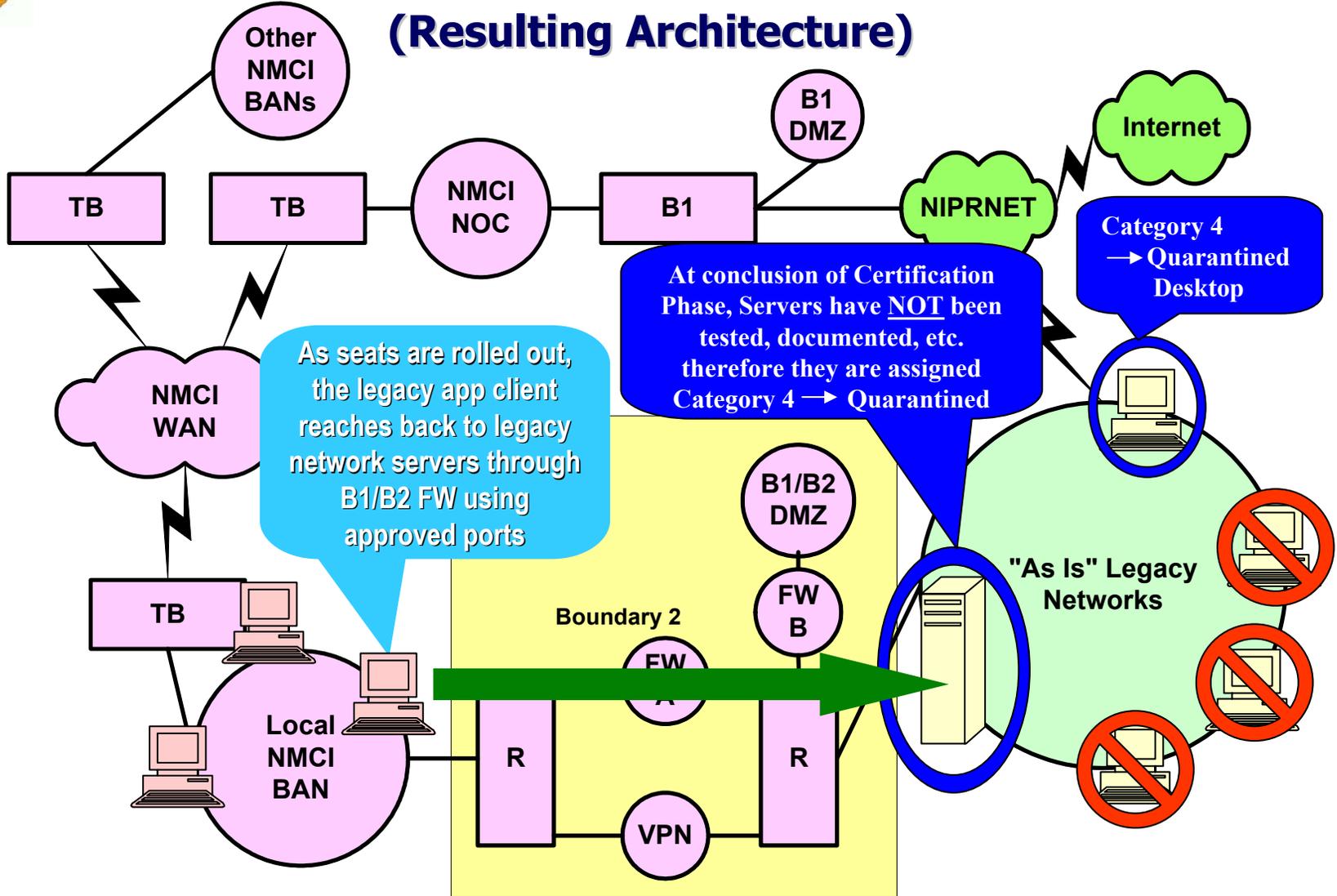
## (Beginning Architecture)





# NMCI Certification

## (Resulting Architecture)



- Elimination/Migration Quarantined Client Applications
- Server Consolidation/Migration within NMCI Network



# Legacy Application Certification Process Comparison

## Original NCARP Process

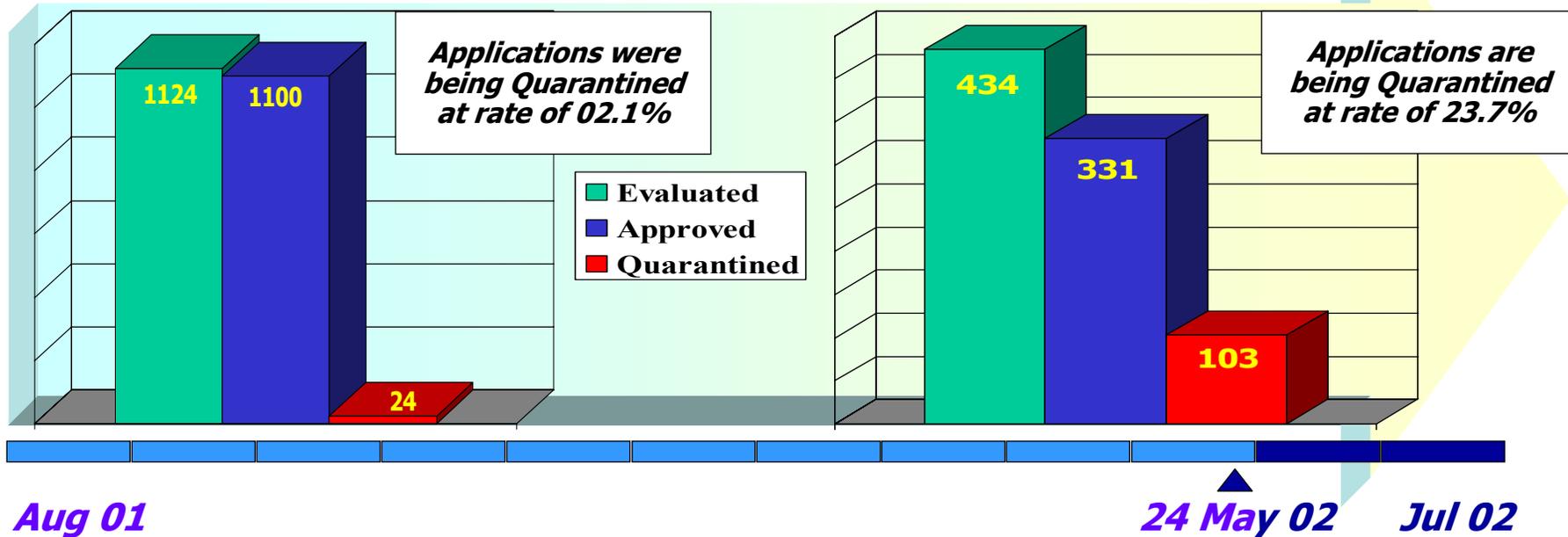
9 Months – 4, 279 Seats across 9 Sites

Applications evaluated: 1124

## Current Rapid Deployment Process

2 Months – 5,048 Seats across 21 Sites

Applications evaluated: 434 Pending: 322



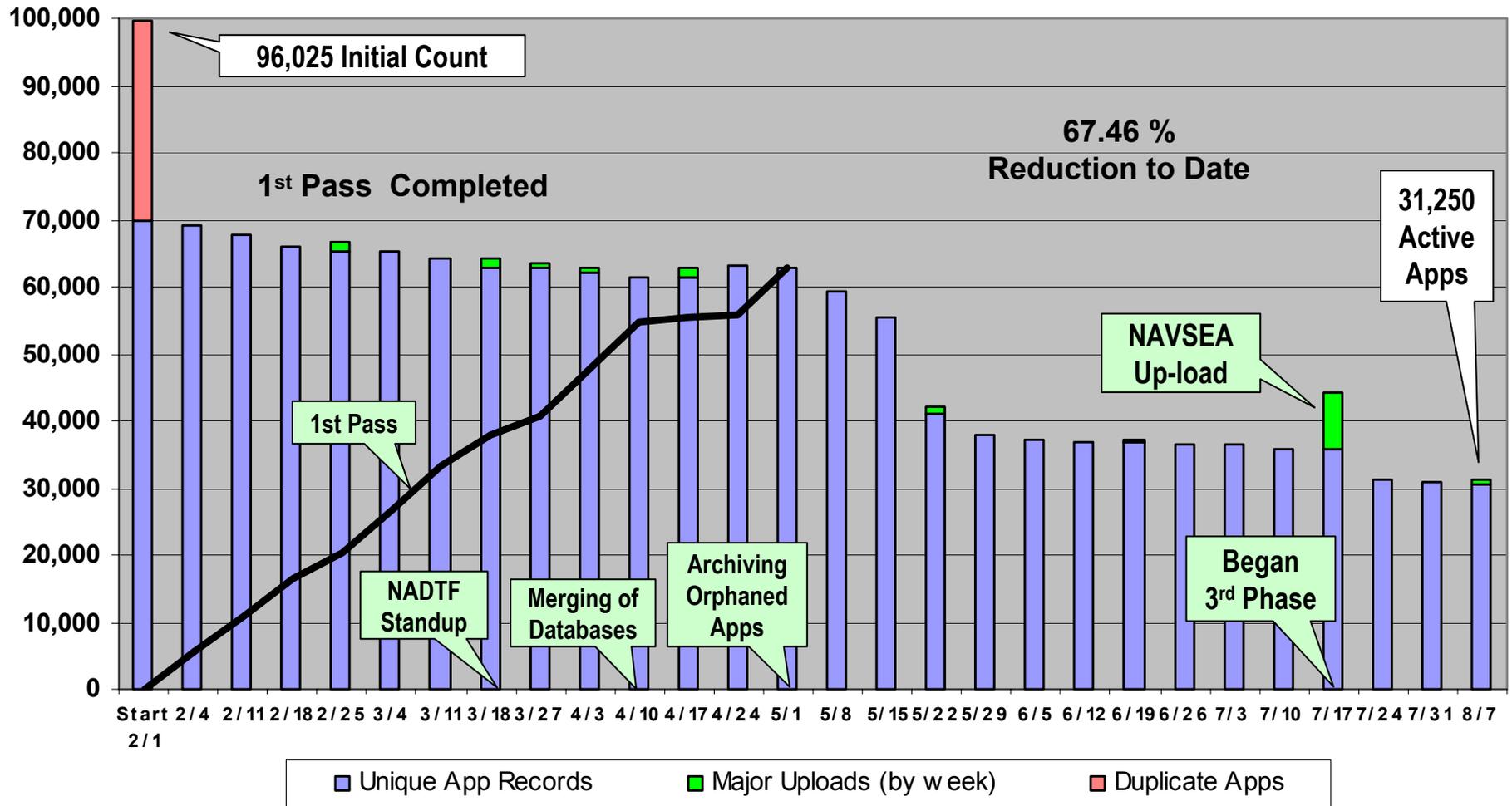
### Notes:

- Process change with Promulgation of Director NMCI MSG, 242225Z MAY 02
  - Charts show throughput of differing processes over DIFFERENT periods of time
- With recent GPO setting update and B2 policy review anticipate 10-15% success rate increase.



# ISF Tools Db Cleanup

## Reduction of Applications





# Quarantine Reduction

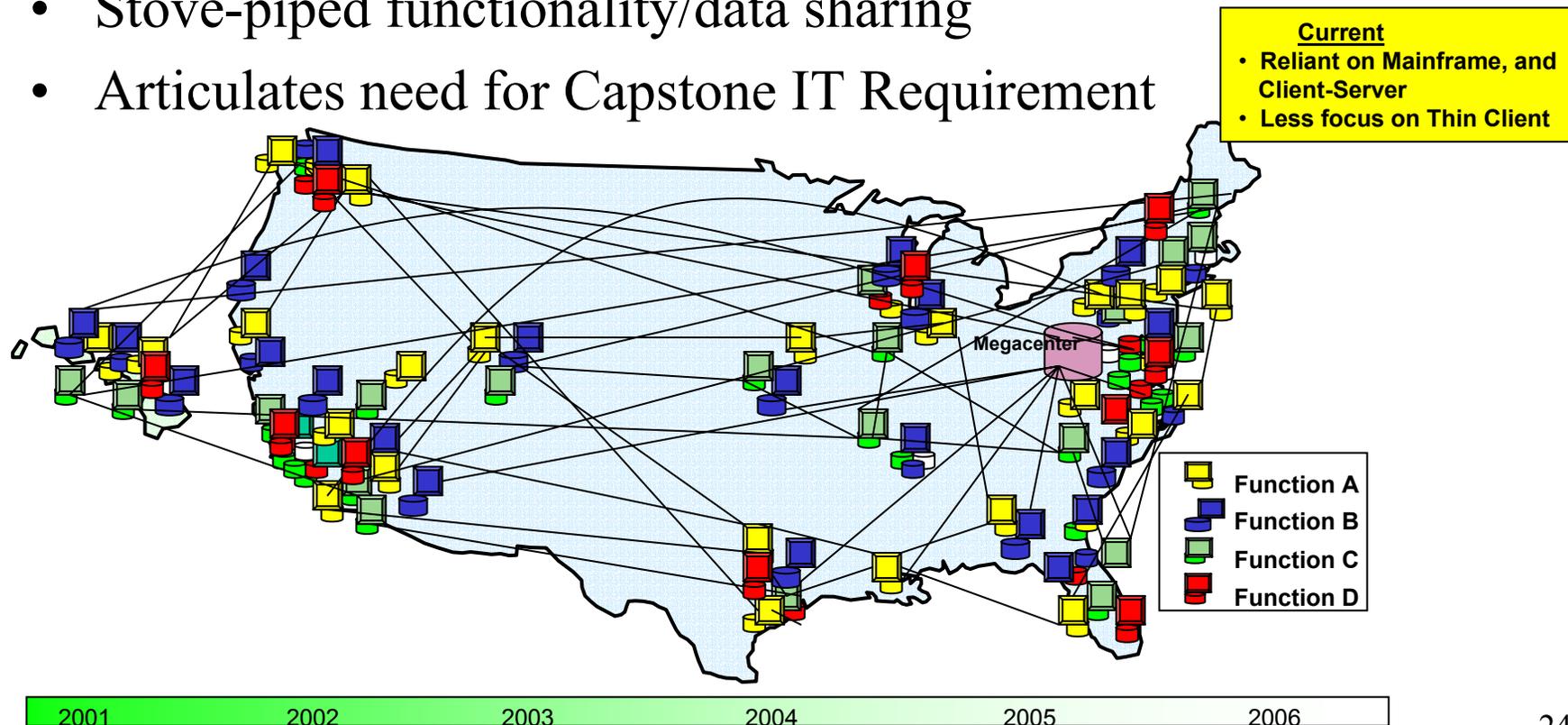
- Validate Reasons for Application failure (W2K, F/W, GPO)
- Applications that require re-engineering remain Kiosked
- Standardize List of Navy Applications
- FAM review and evaluation of Quarantine applications
- ISF accountable to provide access and solutions to connect legacy applications
- Changes to GPO and F/W as required to support enterprise applications



# Application Architecture Evolution

## *Today: Each Application an Independent End-to-end Solution*

- Applications reliant on dedicated databases, servers, and mainframes
  - And will be until NMCI communications infrastructure is in place
- Stove-piped functionality/data sharing
- Articulates need for Capstone IT Requirement

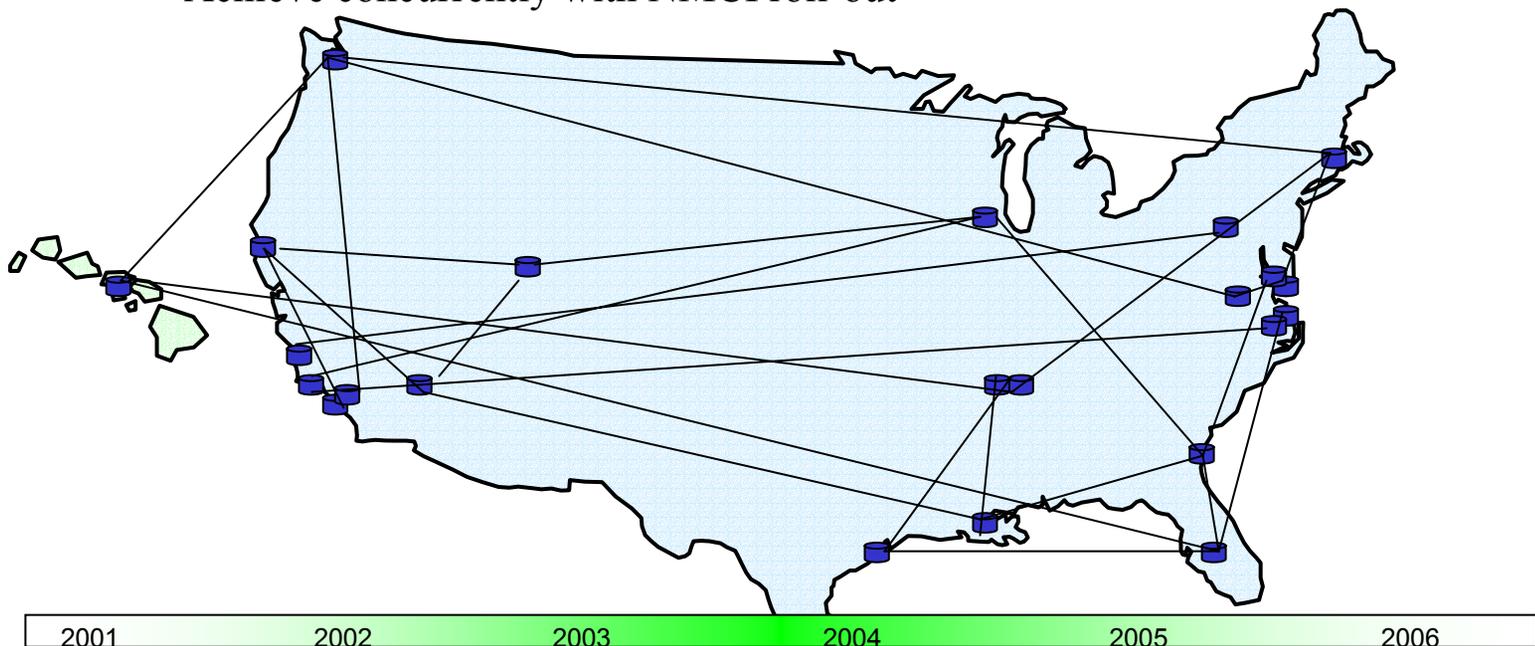




# Application Architecture Evolution

## *Tomorrow: Transition to Interdependence*

- Guaranteed quality of service from the communications infrastructure supports transition to interdependence with shared processors and data bases
- Transition begins with NMCI roll-out
  - Geographic Server Farms for NMCI Gold Disk applications
  - Transition application servers to NMCI server farm locations
  - Still dedicated databases, and in some cases, terminals
  - Does not require restructure of applications
  - Achieve concurrently with NMCI roll-out

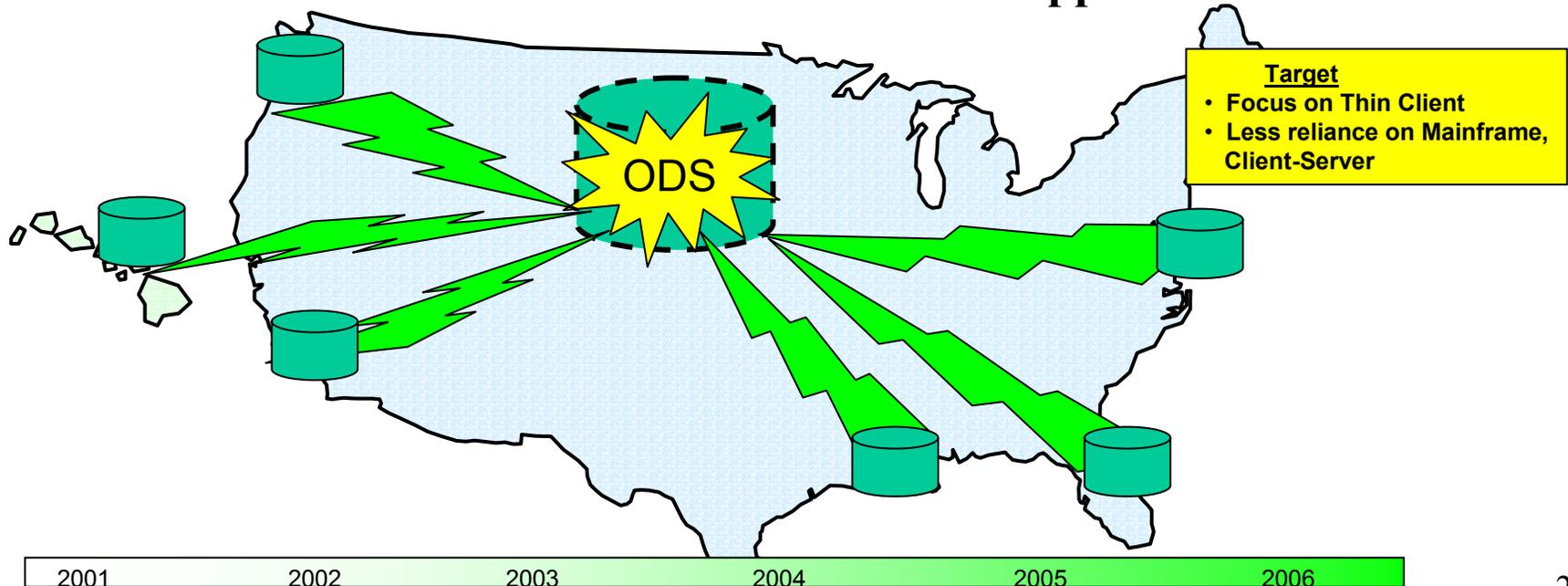




# Application Architecture Evolution

## *Future: Web-Service Centric*

- **Services provided in three layers**
  - Business rules (Application specific)
  - Data (Enterprise)
  - Presentation layer (Enterprise)
- **Single Virtual Operational Data Store and Business Rules Repository**
  - Replicated at NOCs
  - Applicable to all business systems and non-real time tactical systems
- **No dedicated databases or terminals for web applications**





# Current Reality

Customers need interoperable systems

Functional organizations deliver solutions through functional stovepipes

Customers get non-interoperable systems

SECNAV, CNO, CMC, Operational Forces								
Weapons Systems	Intel	C3	Logistics	Training	R&D	Medical	Personnel	Financial
<b>Functional Requirements &amp; Funding</b>								
<b>Systems Planning</b>								
<b>Applications</b>								
<b>Computing Platforms</b>								
<b>Networks</b>								
<b>Workstations</b>								
SECNAV, CNO, CMC, Operational Forces								



# Operators Require?

**Interoperability**

**Bandwidth**

**Security  
&  
Information  
Assurance**

**Reliability**

**End-to-End  
Capability**

**Scalability**



# Operations Require

**... whether war fighting,  
war fighting support or  
commercial**

- **End-to-End Capability**
- **Interoperability**
- **Security / Info Assurance**

**These Principles must be established & complied with  
in the Acquisition, Requirements and PPBS Processes**



# **What is the Goal ?**

- Achieve Network-Centric Operations & Information Superiority**

## **How can this be achieved ?**

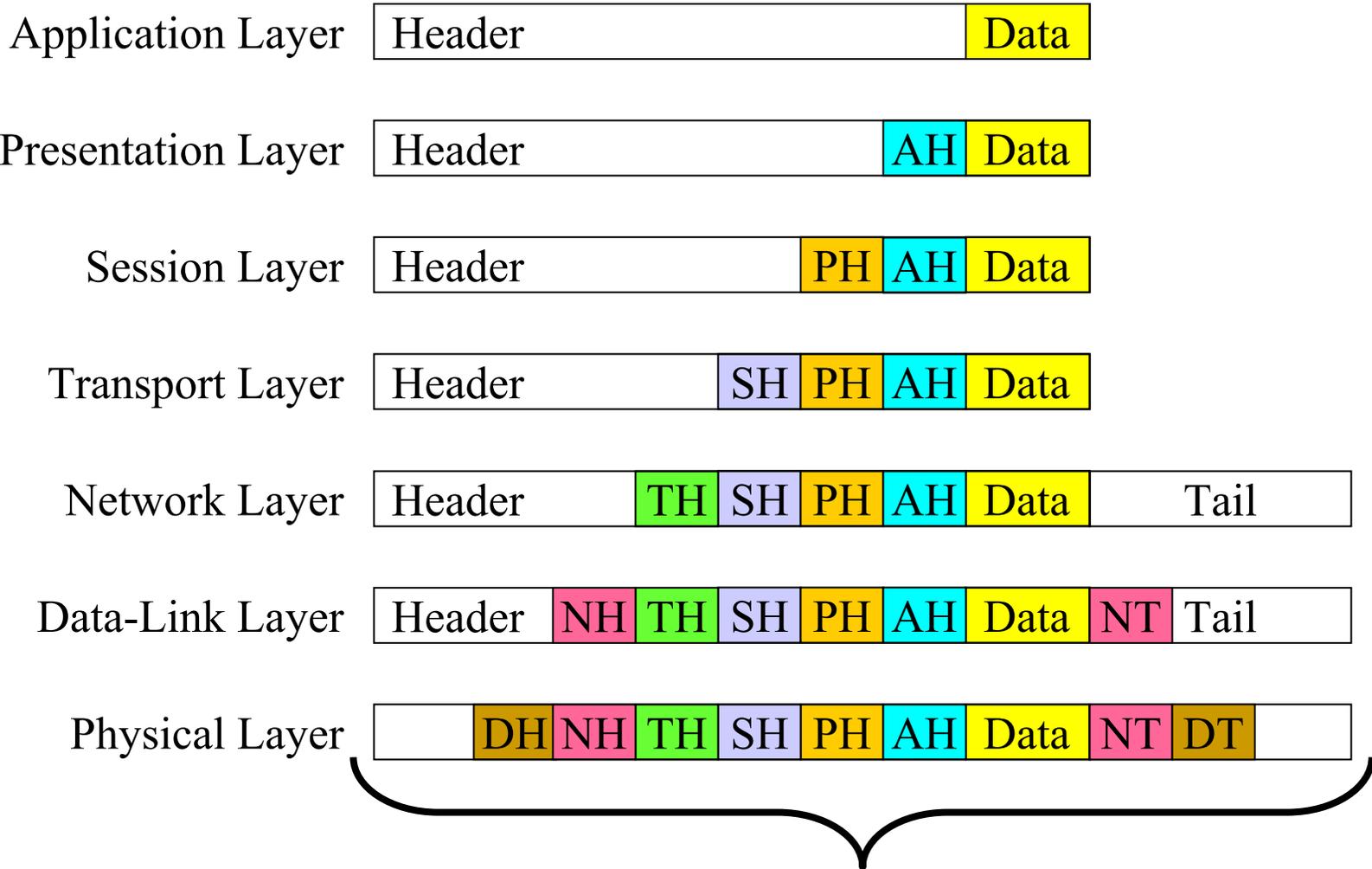
- By placing all Info on a Network and**
- Providing Access to the Network**

## **What is a Network ?**



# Network - OSI Model

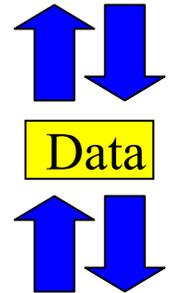
## Open Systems Interconnect (OSI) Model



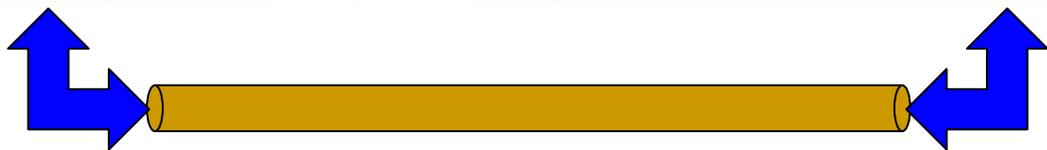
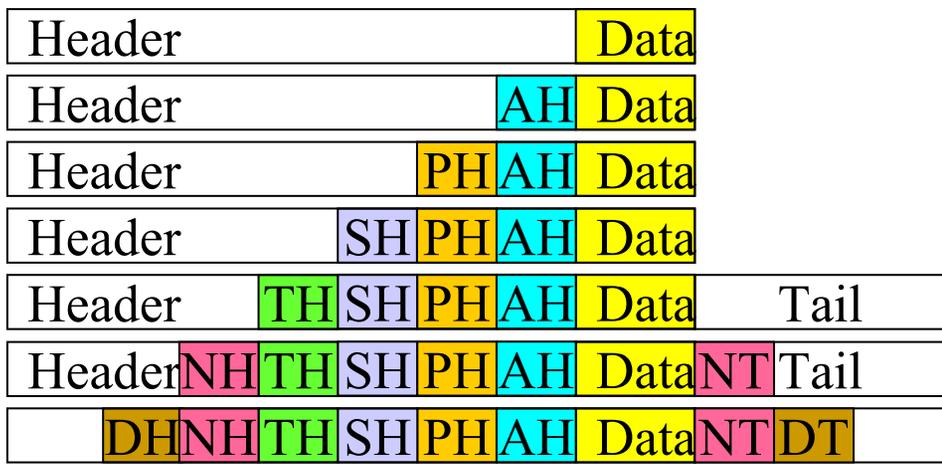
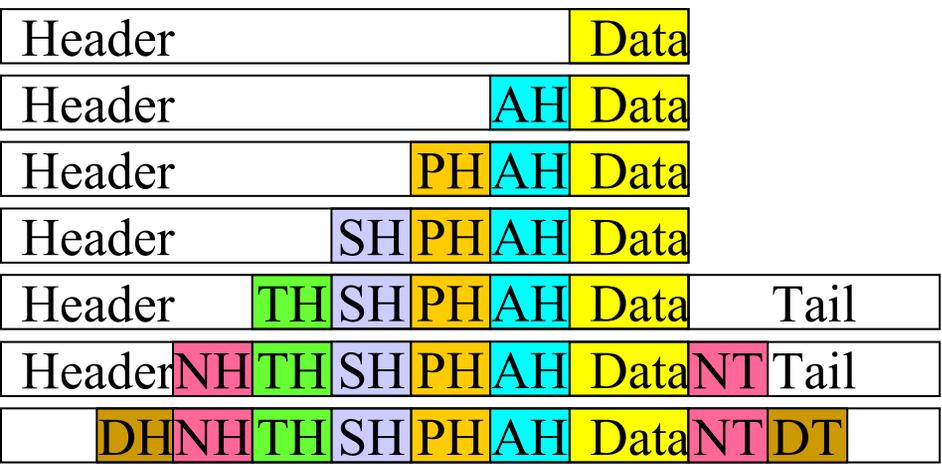
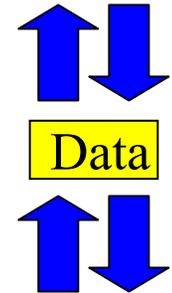


# End-to-End Capability

Information  
Voice, Video or Text



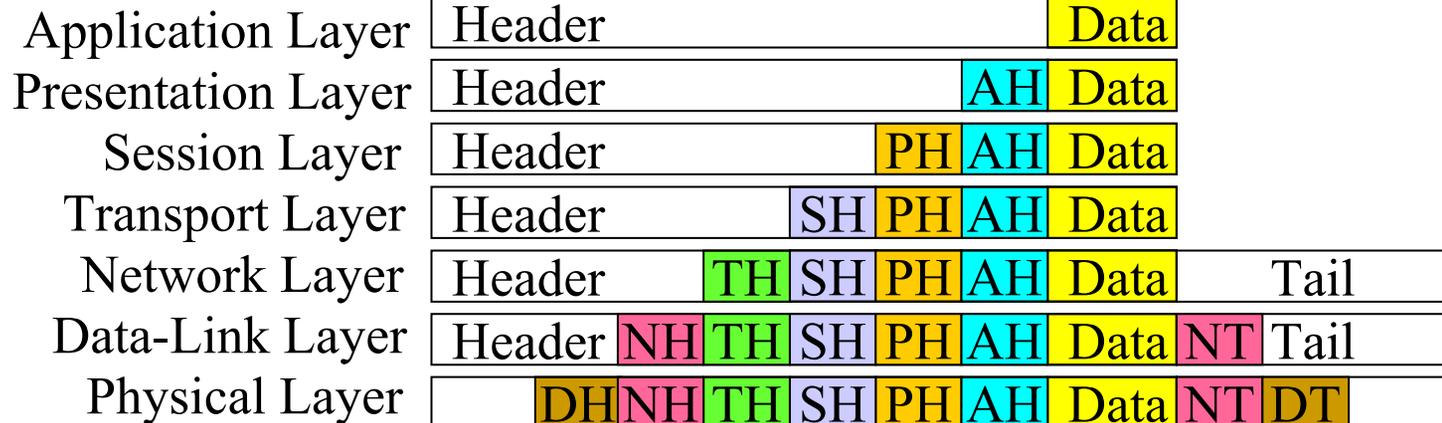
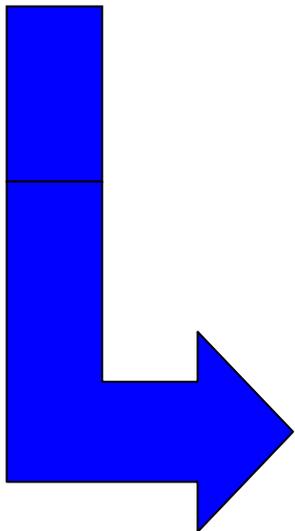
Information  
Voice, Video or Text





# OSI Model

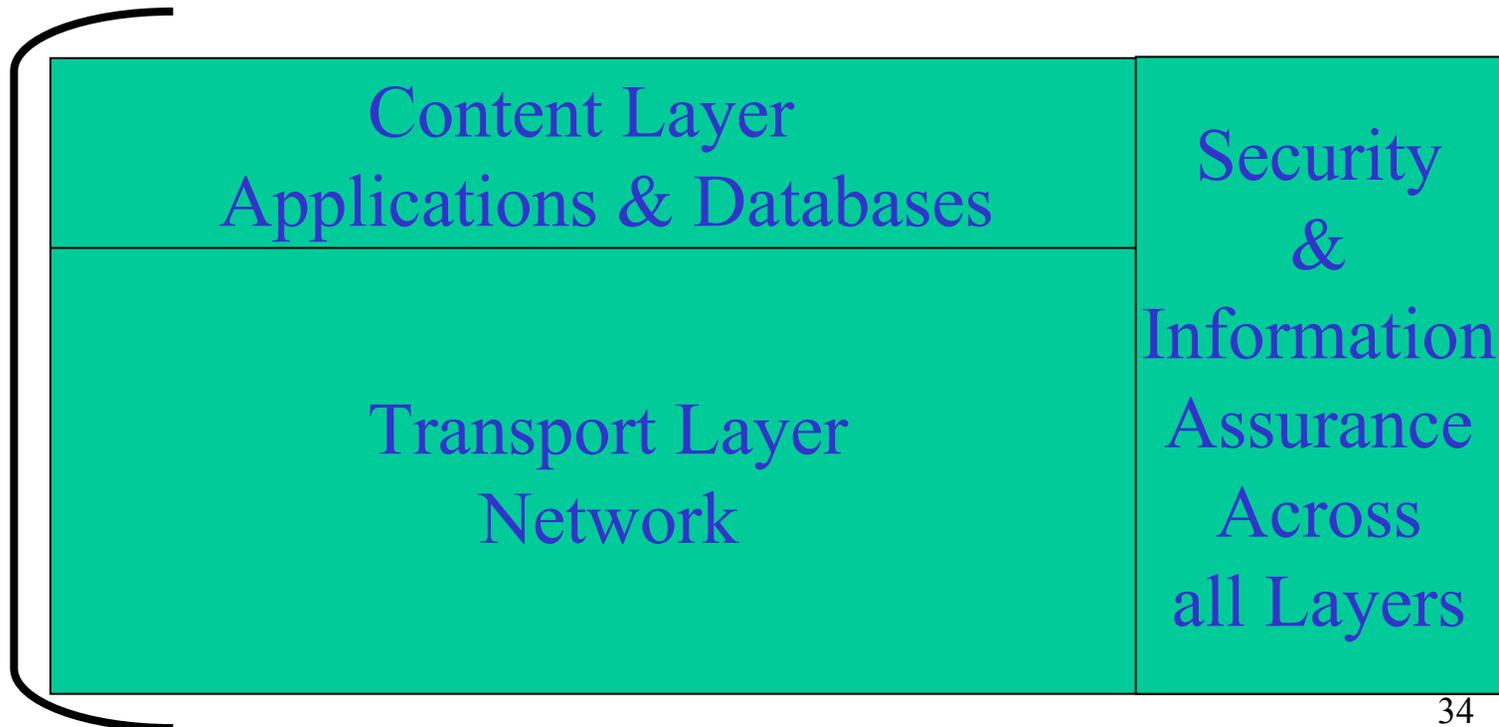
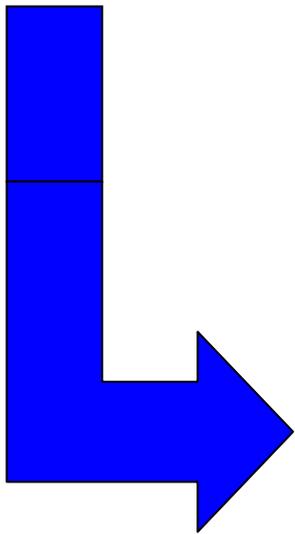
**Each Layer requires:  
Interoperability  
Security / Info Assurance**





# OSI Model

**Each Layer requires:  
Interoperability  
Security / Info Assurance**





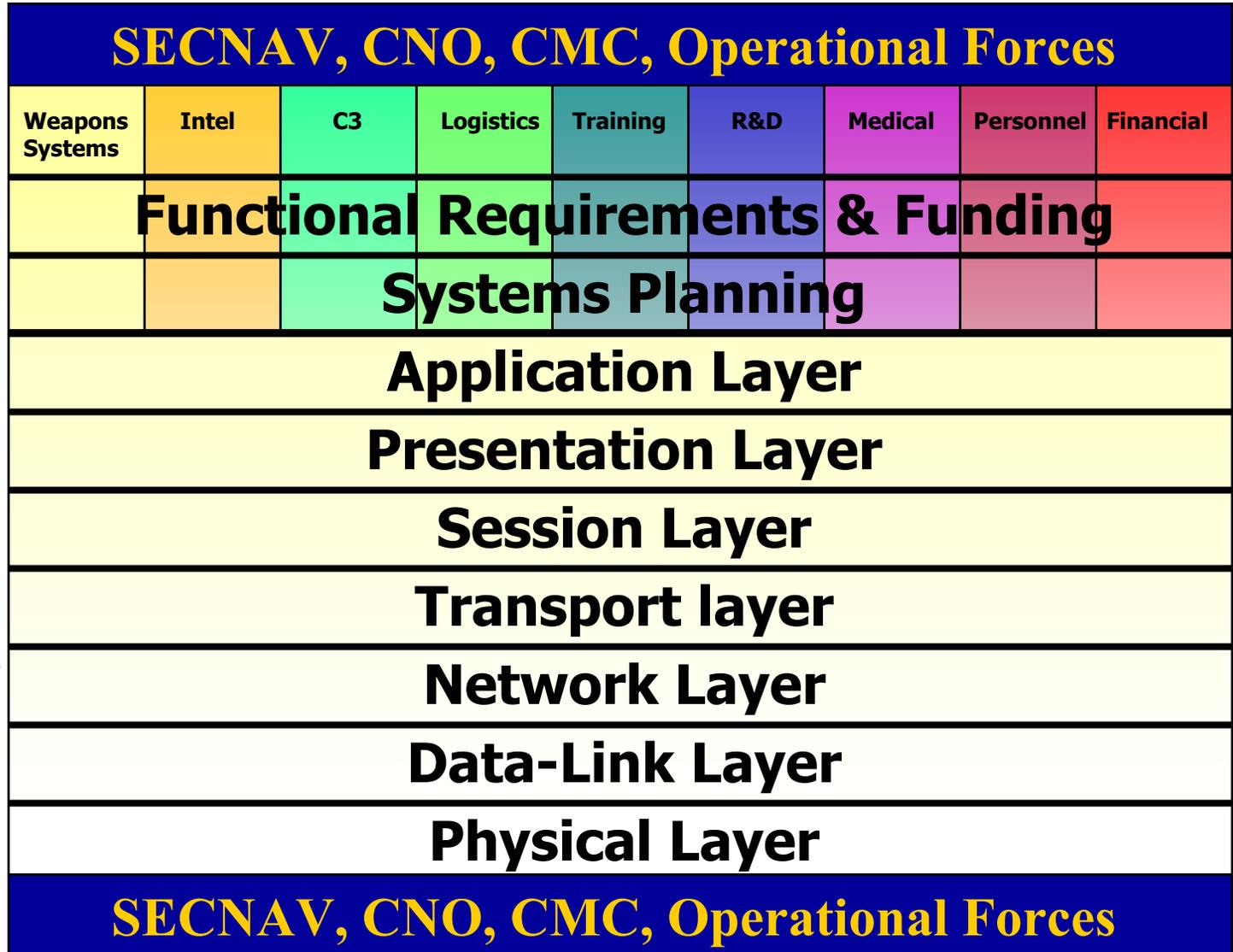
# NIO Vision

Customers need interoperable systems

Sponsor's retain functional requirements and funding of functional area solutions

Sponsor's functional requirements developed under CIO oversight as a DON Enterprise "utility" solution

Customers get interoperable systems





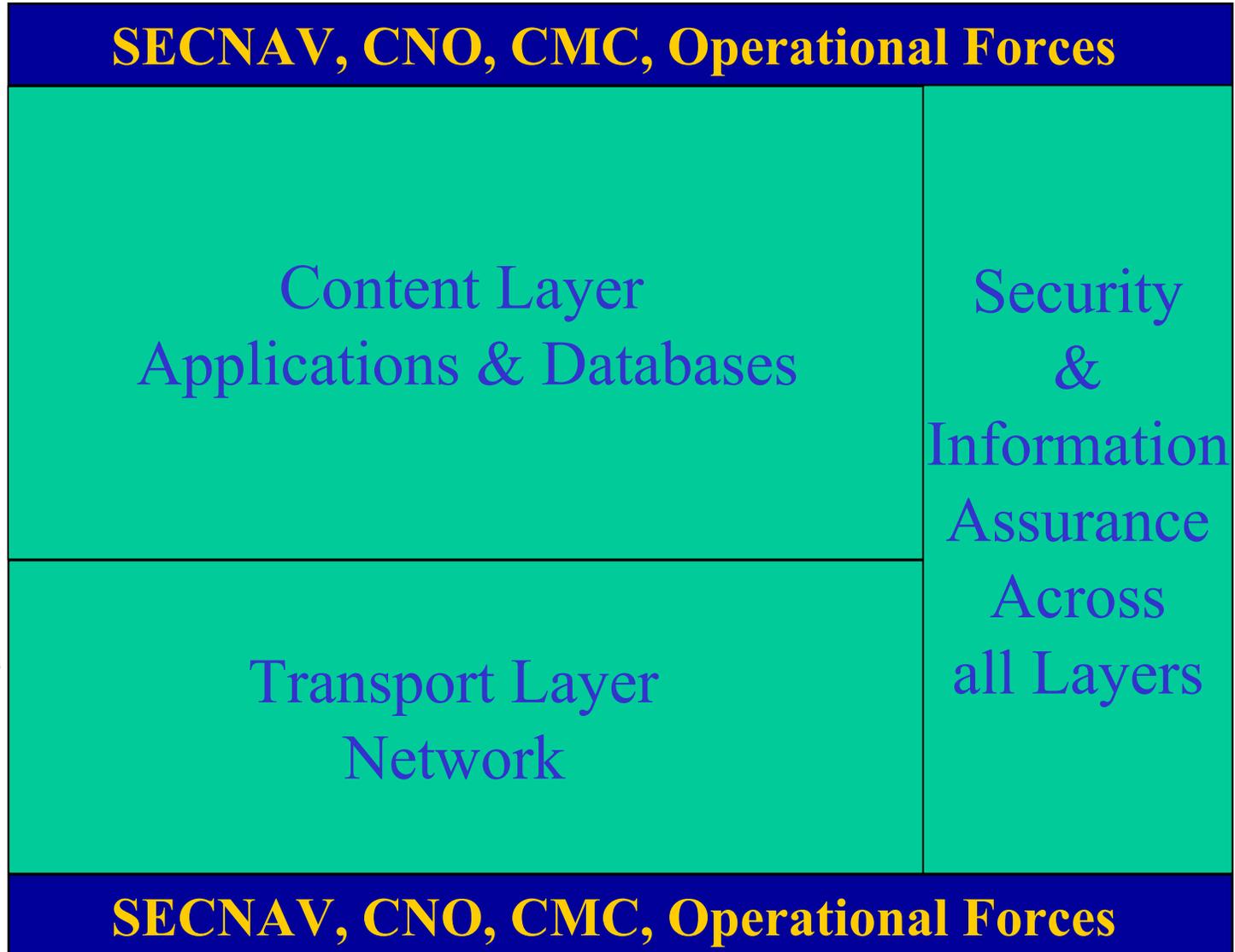
# NIO Vision

Customers need interoperable systems

Sponsor's retain functional requirements and funding of functional area solutions

Sponsor's functional requirements developed under CIO oversight as a DON Enterprise "utility" solution

Customers get interoperable systems





# Definitions .....

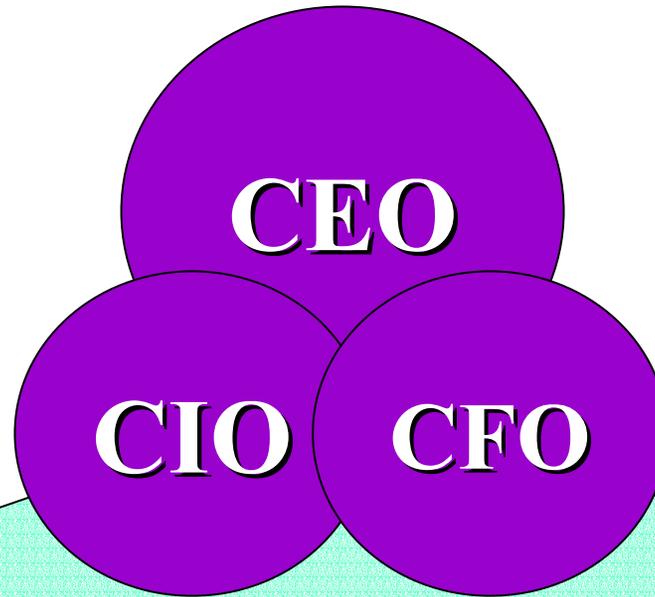
FORCEnet is:

“The operational construct and architectural framework for Naval Warfare in the Information Age which **integrates** Warriors, Sensors, Networks, Command & Control, Platforms and Weapons into a networked, distributed combat system, scalable across the spectrum of conflict from seabed to space and from sea to land.”

Source: Strategic Studies Group XXI Brief to CNO 23 July 2002



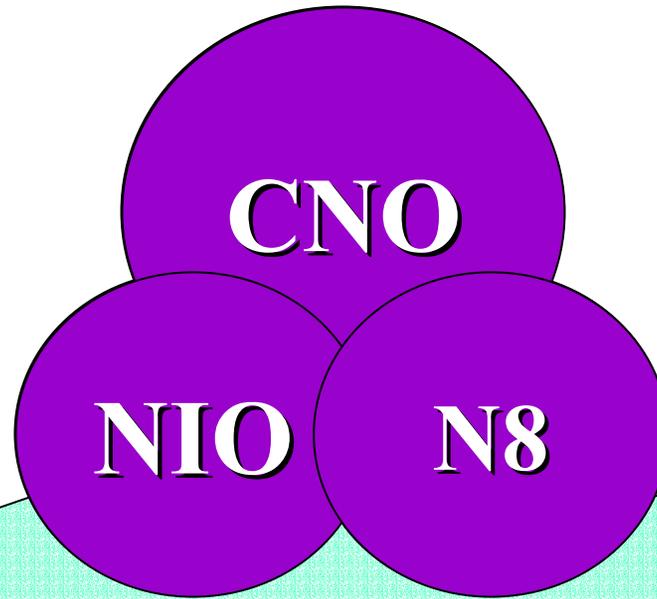
# Accountability – In Business Enforcement



**BUSINESS PROCESS IMPROVEMENT  
THROUGH  
INFORMATION TECHNOLOGY**



# Accountability – In Navy Enforcement



**WARFARE PROCESS IMPROVEMENT  
THROUGH  
INFORMATION TECHNOLOGY**