

# TechNet 2015

*Cyber Convergence*

CIOG6.ARMY.MIL



U.S. ARMY



CIO/G-6

**ENABLING  
SUCCESS**

For Today and Tomorrow

**Mr Gary Wang**

*Deputy Chief Information Officer / G-6*



**27 August, 2015**



# Agenda



- **Mission, Vision**
- **Network Topography**
- **Funding**
  - -DISA partnership
- **Cloud**
- **Mobility**
- **Cybersecurity**
- **Q & A**



U.S. ARMY

# Vision, Mission, Role



## Network Vision

A secure, integrated, standards-based environment that ensures uninterrupted global access and enables collaboration and decisive action throughout all operational phases across all environments.

## CIO/G-6 Mission

CIO/G-6 Leads Army network modernization to deliver timely, trusted and shared information for the Army and its mission partners.

## CIO/G-6 Role

CIO/G-6 Defines overall Army network modernization plans and recommends priorities for the resourcing of network modernization activities.

**Enabling Success For Today and Tomorrow**



# Army Network of Tomorrow

## Vision

A network that is secure, integrated, standards-based, which ensures uninterrupted global access and enables collaboration and decisive action throughout all operational phases across all environments

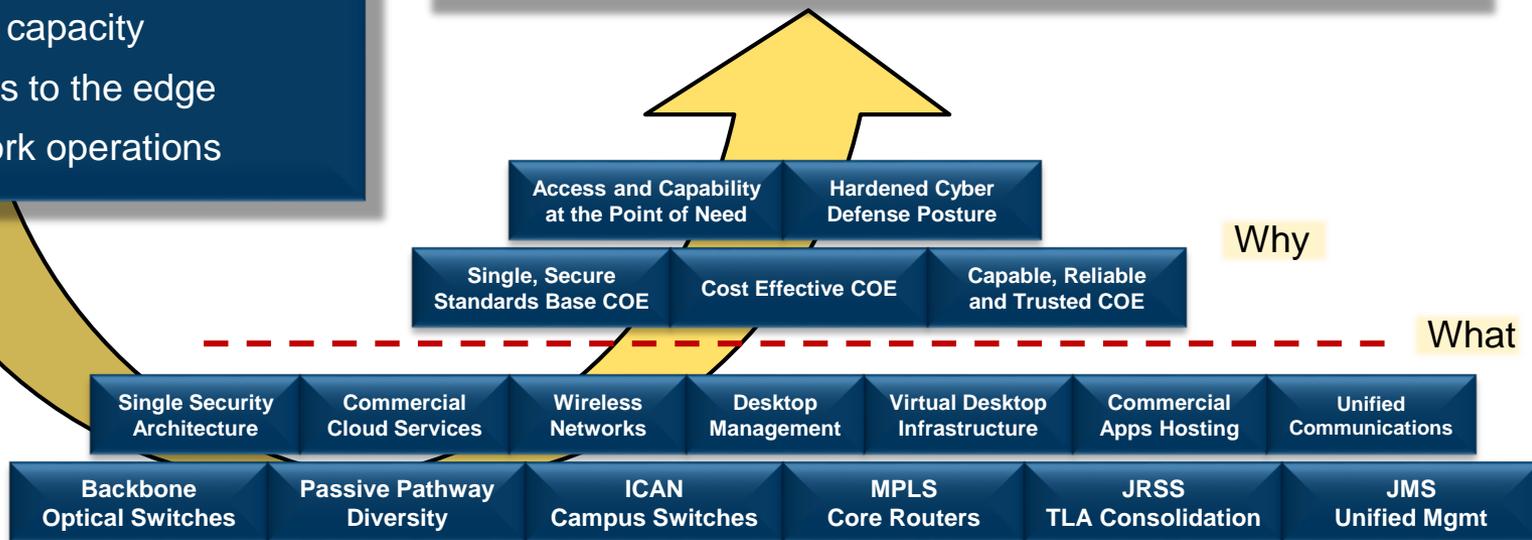
## Lines of Effort

- Provide signal capabilities to the force
- Enhance cyber security capabilities
- Increase network capacity
- Deliver IT services to the edge
- Strengthen network operations

## Operational Outcomes

- Joint and Mission Partner capable
- Distributed, uninterrupted Mission Command
- Assured services to the user – anywhere, anytime
- Maximized security
- Resource efficient, Scalable
- Live/Virtual/Constructive training
- Institutional and operational synergy
- Effective Land Cyber operations

## Key Network Initiatives





# Lines of Effort



## Provide Signal Capabilities to the Force

1.1 Align force structure

1.2 Equip force

1.3 Update doctrine

1.4 Align training and training support capability



## Enhance Cyber Security Capabilities

2.1 Minimize attack surface, establish physical path diversity, strengthen data defense

2.2 Deploy passive & active cyberspace defense capabilities

2.3 Improve cyber-sensing infrastructure, harness big data & increase info sharing



## Increase Network Throughput and Ensure Sufficient Computing Infrastructure

3.1 Implement End-to-end transport infrastructure

3.2 Transition from disparate data processing

3.3 Standardize suite of centrally managed EUDs

3.4 Sync deployable & fixed network



## Deliver IT Services to the Edge

4.1 Plan for global Unified Capabilities

4.2 Transition to Unified Capabilities

4.3 Integrate into tactical network



## Strengthen Network Operations (NetOps)

5.1 Converge to single IT enterprise, reduce complexity

5.2 Define spectrum analytic reqts

5.3 Centralize oversight of critical assets, integrate mgmt/execution decisions

5.4 Enhance & extend incident response, audit, cybersecurity mgmt & SA services

5.5 Develop CONOPS

INTEGRATED NETWORK

COMMON OPERATING ENVIRONMENT

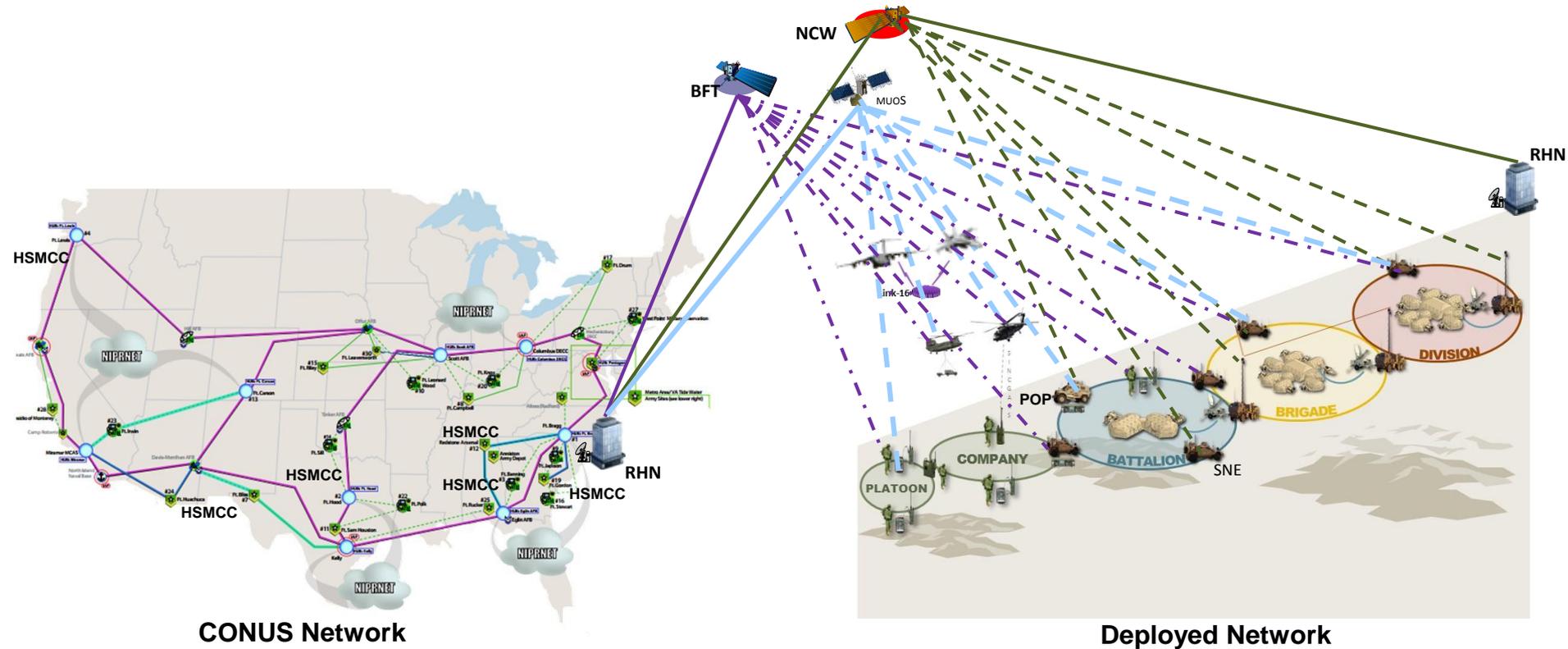
SIMPLIFIED, PROTECTED AND JOINT INTEROPERABLE NETWORK

AGILE EXPEDITIONARY COMMAND POSTS

ENHANCED HOME STATION, TRAINING & READINESS



# Network Topography



**One Army Network**



# Current Model Applied to Federal Government



## Cloud Computing Services

### Software as a Service (SaaS)

- Citizen Engagement (Wikis, Blogs, Data.gov)
- Government Productivity (Cloud

### Platform as a Service (PaaS)

- Database /Database Mgmt Systems
- Developer / Testing Tools
- Virtual Environments

### Infrastructure as a Service (IaaS)

- Computing
- Storage
- Application hosting

## Federal Government Considerations

### Security & Data Privacy

Offer different levels of security and data privacy based on the application and nature of the services provided.

Potential standardize Low, Med and High categories for Simplicity.

### Delivery & Operations

Enable adoption of Cloud Computing services in different Cloud models including Public, Private, Hybrid and Community models.

### Interoperability & Integration

Develop interoperability standards in conjunction with the industry to provide interoperability at the data infrastructure, platform and application levels.

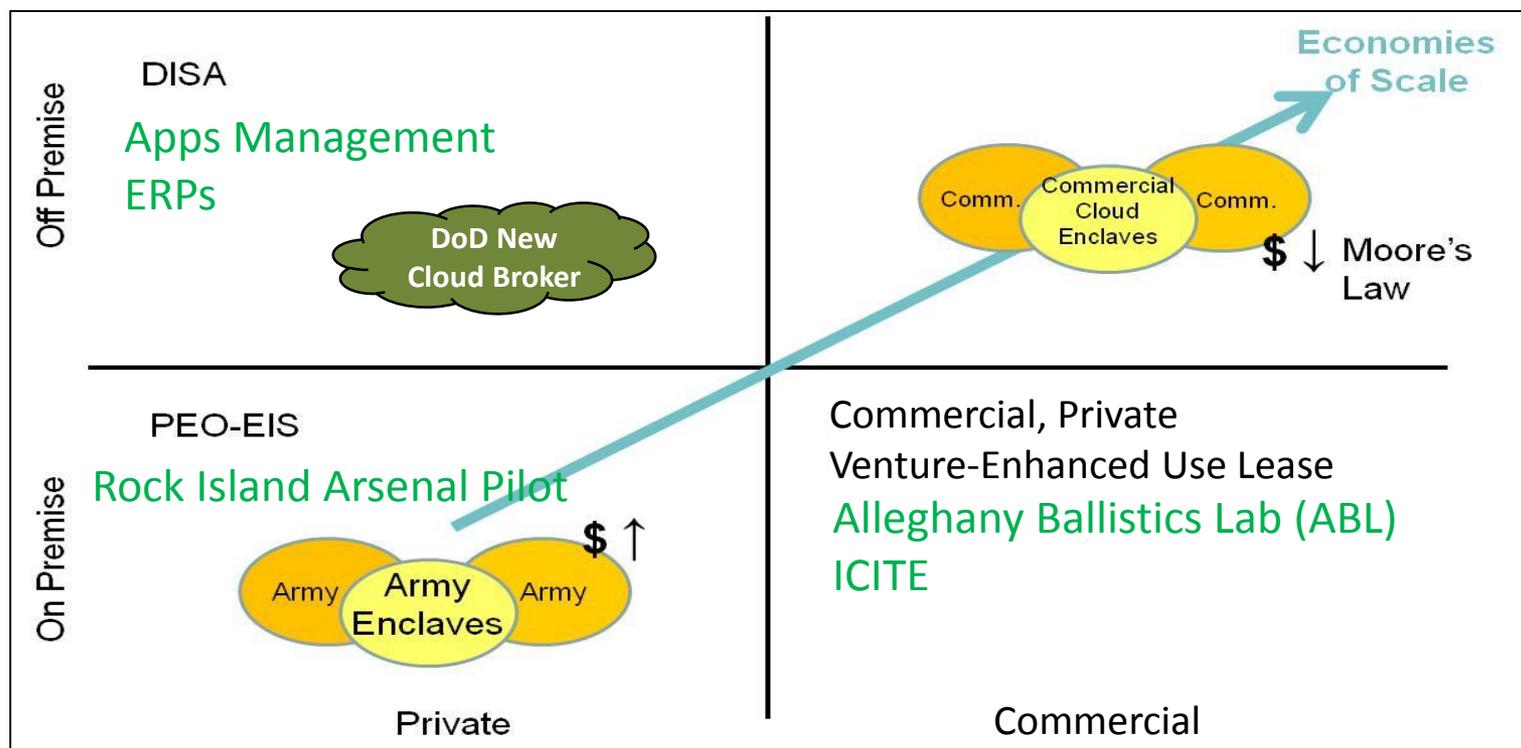


# Commercial Cloud



- Two commercial cloud pilots
- First pilot for public facing websites
- Designed to establish cost baseline for services and security models
- Second pilot for NIPRNET-level services

## Data Center Consolidation Landscape





# Mobility



<https://itunes.apple.com/us/artist/tradoc-mobile/id960437358>

<https://play.google.com/store/apps/developer?id=TRADOC%20Mobile&hl=en>

<https://www.windowsphone.com/en-US/store/publishers?publisherId=US%2BArmy%2B>

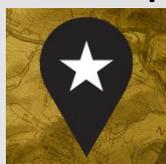
## Installation



## Organizational



## Leadership



## Maintenance



## (SHARP)



14+ Installations

## Transportation



## Finance



## AER



## Retirees



## Health & Fitness



## Compensation & Benefits



## Education



## Public Affairs

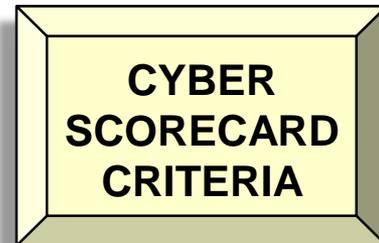


## Doctrine

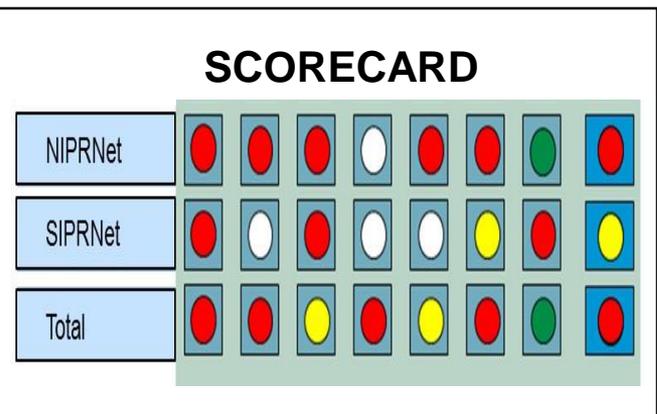




# DoD Cybersecurity Scorecard



- 1) Every Web Server on SIPRNet and Private Web Server on NIPRNet Must Use PKI for User Authentication
- 2) Remove Windows XP Operating System Software from Entire SIPRNet & NIPRNet Inventory
- 3) Remove Windows Server 2003 Operating System Software from Entire SIPRNet & NIPRNet Inventory
- 4) Evaluate and Approve Systems, Fix Vulnerabilities, Perform Regular Security Control Testing



- 5) Move all Outward Facing Servers to Approved DMZs
- 6) Every Computer Configured to DoD Security Standard
- 7) Ensure Every System Administrator Logs On via PKI
- 8) Implement Host Based Security System
- 9) Ensure Every User Logs On via PKI
- 10) Every Computer Properly Patched



U.S. ARMY



# Questions



# TechNet 2015

*Cyber Convergence*

CIOG6.ARMY.MIL



U.S. ARMY



CIO/G-6

## ENABLING SUCCESS

For Today and Tomorrow

## Mr Gary Wang

*Deputy Chief Information Officer / G-6*



27 August, 2015