Army Network Campaign Plan, Architecture and Data

Gary W. Blohm, SES
Director, CERDEC CP&I
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 Leads Army network modernization to deliver timely, trusted and shared information for the Army and its mission partners.

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
Implementation Guidance Near-Term
- Describes activities in year of execution
- Reflects acquisition, resource and mission reality
- Guides design & development of the next network capability

Implementation Guidance Mid-Term
- Focuses on network capabilities
- Influences program resource planning within Program Objective Memorandum (POM)

The Network Modernization Execution Order (EXORD)
Execution guidance and roles and responsibilities for near-term activities supporting the Army Network Campaign Plan. It establishes investment priorities, milestones, and deliverables to support incremental network modernization.
Army Network Campaign Plan

Purpose

- Defines CIO/G-6’s Vision, Mission and Role’s for the Army Network
- Clarifies Strategic Environment Facing the Army
- Introduces CIO/G-6 Lines of Effort (LOE), Desired End States and Supporting Objectives
- Provides an Army Network Initiatives Roadmap
Near Term (2016-2017)

NETWORK NEAR-TERM CAPABILITIES

- Common Operating Environment (COE)
- Infrastructure Modernization & Network Consolidation (MPLS)
- Cyber Attack Surface Reduction (JRSS)
- Single Service Management System (JMS)
- Data Center Consolidation & Application Rationalization/Migration
- Unified Capabilities (UC) RFP
- Government/Commercial Cloud
- Refine the Role of Cyber Workforce
- Home Station, En Route and Early Entry Command Post
- Command Post Computing Environment (CP CE)
- Expeditionary Mission Command

BIG IDEAS

- **Common Operating Environment:** standardization across computing environment with simplified user experience
- **Cloud-based collaboration**
- **Bandwidth** to meet the demand of the current and future Army
- **Extending Enterprise Services** into the Tactical Edge
Mid Term (2018-2022)

NETWORK MID-TERM CAPABILITIES

- Unified Capabilities as a Service (UCaaS)
- Secure Mobile Solutions / 4G LTE and Wireless (WIFI)
- Leverage Big Data Analytics
- Mission Partner Environment
- Transportable Tactical Command Communications (T2C2)
- Data radios to support Company and below key leaders
- Command Post Computing Environment v2 and v3
- Mounted CE with a common software foundation and development kit for COE v3 with interoperable apps and widgets
- Synchronize and integrate continuous monitoring solutions
- Access management based on user identity attribute size cryptology capabilities

BIG IDEAS

- **Wireless** networks and Bring Your Own Device
- **Unified Capabilities** (single device delivering voice, video, and computing capabilities)
- Collaborate with unified action partners on any trusted device globally
“Technology consistently impacts warfare and there have been significant advances in warfare and equipment …..Some of these advances include: the proliferation of drones both for attack and reconnaissance; the ability to know where every combat vehicle is located on the battlefield through Blue Force Tracking; the evolution of mission command software (from acetate map boards to large screen displays); and new communications gear that allow soldiers to communicate beyond line-of-sight. …..We expect that as innovation accelerates, even greater advances will emerge over the next 25 years.”
LandWarNet (LWN) 2020
Enterprise Architecture

Guidance Documents
- LWN 2020 & Beyond Enterprise Architecture
- Annex A Technical Guidance
- Annex B COE

Reference Architectures
- Army Information Architecture
- Network Capability Sets

Authoritative/Requirements Documents
- Army Network Campaign Plan (ANCP)
- ANCP Implementation Guidance
- NCS FY15 EXORD

Operational CS Design Books
- CCI/Installation CS Reference Architecture

Army Data Strategy integrated within Enterprise Architecture

Unity of Effort
Army Cloud Computing Strategy

The Army Cloud Computing Strategy is Designed to:

- Establish and communicate the Army’s vision and approach for transitioning to a cloud-enabled network
- Improve mission and business effectiveness
- Increase operational information technology (IT) efficiencies
- Protect Army data and infrastructure

The Army Cloud Computing Strategy Clarifies:

- Strategic intent, guiding principles, and identifies strategic imperatives and enabling objectives to transition the Army to cloud computing within all defined computing environments.

Commercial Cloud Services Provider Policy Guidance in Development

Released 25 March 15
Army Directive 2009-03
(Army Data Management)

- Declares that "Data is a strategic asset and must be managed as such"
- Assigns responsibility to CIO/G-6 to establish and oversee the Army Data Management Program (ADMP)
- Creates the position of Chief Data Officer (CDO)
- Creates the Army Data Board (ADB)
- Creates the position of Army Data Stewards (ADS)
Document Evolution and Linkages

Cloud Services
AQ Vehicle
Levels 3-5
PEO-EIS

CNDSP CONOPS
2A/ARCYBER

Army Data Policy

6QTR FY16 CIO/G6 Data Policy

Quality Metrics

Army Data Management Program – Management Overview
FY 16 CIO/G6 ADEP Vol 1

UNCLASSIFIED
Army Data Strategy Overview

- **Purpose**
  - **Establish** and communicate the Army’s vision and strategy for the **sharing of data and information**; reduce **redundancy** of data and increase **IT efficiencies**
  - **Complies with DoDI 8320.02** (and DRAFT DoDI 8320.ff) and **aligns with DoD IEA**
  - **Codifies COE and COE Implementation** by providing specific, rules based guidance via the AIA

- **Scope:** Applies to all Army IT applications, systems or databases within the Army Portfolio to **guide and inform related operational activities and** realize the five strategic imperatives

- **Guiding Principles**
  - Data is an enterprise **asset**
  - Data is **not** the same as **information**
  - Effective decision-making requires effective **information sharing**
  - Data must be **visible and accessible** to authorized users
  - Accessible **regardless of location**
  - Data must be **protected**
Army Data Strategy Overview (cont’d)

- **Strategic Imperatives**: (Army strategy is the same as the DoD strategy. Army strategic imperatives are the same as the DoD goals.)
  - Make data **Visible**
  - Make data **Accessible**
  - Make data **Understandable**
  - Make data **Trusted**
  - Make data **Interoperable**

- **Enabling Objectives**: Numerous underlying activities or initiatives that enable the Army to successfully and effectively share data and information
  - Army Data Management Program (ADMP)
    - Army Data Governance [visible-accessible-understandable-trusted-interoperable]
    - Army Data Integration and Interoperability (via AIA) [understandable – interoperable]
    - Authoritative Data Sources (ADS) [visible – accessible – trusted]
    - Information Exchange Specification (IES) [interoperable]
  - Additional Overarching Enabling Objectives
    - Unique Identifiers [trusted – interoperable]
    - Army Data Quality Management [trusted]
    - Army Data Metrics [understandable – trusted]
    - Army Data Management Guides [understandable]
Data Strategy Interrelationships

**Governance**

- **DoDI 8320.02**
  - VAUTI Goals
  - DSE
  - DISR

- **DIEA**
  - Priority areas
  - Principles
  - Rules

- **CJCSI 6212.01F**
  - NR KPP
  - Certifications

- **AIA**
  - Rules Based
  - Provides policy, guidance and tools to implement information sharing
  - Compliance Testing

- **AR 25-1**
  - Security
  - Standards
  - Certifications

- **DA Pam 25-1-1**
  - Procedures
  - Guidance

- **AD 2009-03**
  - Data is a strategic asset
  - Establishes ADMP, CDO, Army Data Board, Army Data Stewards

**COE Implementation Plan / Integrated Systems Engineering Plan**

**Operational Data**
• **Challenge:** Moving from system-centric to data-centric approach to Mission Command software – focusing on the data layer

• **Payoff:** Making data easier to access/move will facilitate lighter weight application development

• **Tactical Computing Environment (TCE) project** - focuses on Mission Command data needs across the Command Post, Mounted, and Mobile/Handheld Computing Environments (CEs) within the Army Common Operating Environment (COE) initiative

• Computing environment **architecture** improvements and **prototypes** focus on the collection / management / storage / transformation / routing / synchronization of data to facilitate Mission Command in environments with limited computing resources, networks, and staff support
• Software architecture that enables dynamic data exchange and flexible data architectures

- Acknowledges current systems / data models / data stores and provides technical guidance and patterns for integration
- Abstractions and layering approach to allow for diverse / emerging data and software technologies
- Looks at mechanics of exchange as well as transformation of data into information
- Technical guidance on semantic mediation, metadata (time, provenance, interpretation, etc.), and caching to support cross-CE operability
• Developing and evaluating a set of data services to support Mission Command data needs across CEs on all devices, whether connected or disconnected from the tactical network (DIL environment)

  – Used to read, write, modify, delete, subscribe to, and analyze data collected and used throughout the tactical computing environment
  – Addresses a variety of data issues: distribution, caching, storage, synchronization, mediation, access, and schema management

• Knowledge representation and reasoning

  – Cataloging and semantic metadata to store and represent knowledge (data becomes information)
  – Dynamic discovery / alignment of data without prior knowledge or formatted exchange
  – Advanced data queries and analysis tools
CIO/G6 Website
Back Up
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