DEPARTMENT OF THE ARMY
WASHINGTON DC 20310

OCT 20 2010

SAIS-AEA

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Common Operating Environment Architecture Guidance

1. References:

a. Memorandum, Vice Chief of Staff of the Army (VCSA), subject: Achieving Army Network and Battle Command Modernization Objectives, dated 28 December 2009

b. Document, CIO/G-6, titled: Common Operating Environment Architecture, (Appendix C to Guidance for 'End State' Army Enterprise Network Architecture), dated 1 October 2010

2. The CIO/G-6, in close coordination with ASA(ALT) Systems of Systems Engineering (SOSE), has developed the Common Operating Environment (COE) Architecture concept, framework and standards for the Army Enterprise Network. In addition, in order to inform Program Objective Memorandum 13-17 investment decisions, ASA(ALT) will publish a complementary Implementation Plan that describes the steps and schedule for bringing Army systems into compliance with the COE Architecture guidance. Henceforth, compliance with the COE Architecture and Implementation Plan will be mandatory for all programs under the purview of the Army Acquisition Executive.

3. The CIO/G-6 and ASA(ALT) are committed to enabling the Army to produce high-quality applications rapidly while reducing the complexities embedded in the design, development, testing and deployment cycle. The COE Architecture and Implementation Plan will provide direction to our industry partners regarding our framework standards. Both documents are considered to be living instruments and will continue to evolve in a coordinated manner in order to keep up with the rapid changes in technology.

4. Our points of contact for this memorandum are: COL Anthony Howard, Sr., (703) 604-2068 or anthony.howardsr@us.army.mil; and Mr. Phillip Minor, (703) 604-7133 or phillip.minor@us.army.mil.

JEFFREY A. SORENSON
Lieutenant General, GS
Chief Information Officer/G-6

Malcolm R. O'Neill
Assistant Secretary of the Army
(Acquisition, Logistics and Technology)

SAIS-AEA
SUBJECT: Common Operating Environment Architecture Guidance

DISTRIBUTION:
PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY

COMMANDER
- U.S. ARMY FORCES COMMAND
- U.S. ARMY TRAINING AND DOCTRINE COMMAND
- U.S. ARMY MATERIEL COMMAND
- U.S. ARMY EUROPE AND SEVENTH ARMY
- U.S. ARMY CENTRAL
- U.S. ARMY AFRICA
- U.S. ARMY NORTH
- U.S. ARMY SOUTH
- U.S. ARMY PACIFIC
- U.S. ARMY SPECIAL OPERATIONS COMMAND
- MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
- U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY STRATEGIC COMMAND
- EIGHTH U.S. ARMY
- U.S. ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL COMMAND (ARMY)
- U.S. ARMY MEDICAL COMMAND
- U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
- U.S. ARMY CRIMINAL INVESTIGATION COMMAND
- U.S. ARMY CORPS OF ENGINEERS
- U.S. ARMY MILITARY DISTRICT OF WASHINGTON
- U.S. ARMY TEST AND EVALUATION COMMAND
- U.S. ARMY RESERVE COMMAND
- U.S. ARMY INSTALLATION MANAGEMENT COMMAND

SUPERINTENDENT, U.S. MILITARY ACADEMY

DIRECTOR
- U.S. ARMY FINANCE MANAGEMENT COMMAND
- U.S. ARMY TEST AND EVALUATION CENTER
- U.S. ARMY RESEARCH LABORATORY
- U.S. ARMY CHEMICAL MATERIALS AGENCY
- U.S. ARMY ACQUISITION SUPPORT CENTER

DISTRIBUTION: (CONT)

PROGRAM EXECUTIVE OFFICER
- AMMUNITION
- AVIATION
- COMBAT SUPPORT AND COMBAT SERVICE SUPPORT
- COMMAND, CONTROL AND COMMUNICATIONS (TACTICAL)
- ENTERPRISE INFORMATION SYSTEMS
- GROUND COMBAT SYSTEMS
- INTEGRATION
- INTELLIGENCE, ELECTRONIC WARFARE AND SENSORS
- MISSILES AND SPACE
- SIMULATION, TRAINING AND INSTRUMENTATION
- SOLDIER

JOINT PROGRAM EXECUTIVE OFFICER:
- CHEMICAL AND BIOLOGICAL DEFENSE
- JOINT TACTICAL RADIO SYSTEM

CHIEF INFORMATION OFFICER
- AVIATION MISSILE LIFE CYCLE MANAGEMENT COMMAND
- CECOM LIFE CYCLE MANAGEMENT COMMAND
- JOINT MUNITIONS AND LETHALITY LIFE CYCLE MANAGEMENT COMMAND
- U.S. ARMY TANK-AUTOMOTIVE AND ARMAMENTS LIFE CYCLE MANAGEMENT COMMAND

CF:
SAAL-ZP
SAAL-ZS
SAAL-ZT
SAIS-ZA
SAIS-AO
SAIS-AEA

Common Operating Environment Architecture

Appendix C to Guidance for 'End State' Army Enterprise Network Architecture

U.S. Army CIO/G-6

1 October 2010

Executive Summary

On 28 December 2009, the Vice Chief of Staff of the Army (VCSA) directed CIO/G-6 to develop 'as is' and 'end state' network architectures to guide evolution of network procurements and enhancements. The *Army Network Architecture Strategy – Tactical* version 1.1, dated 6 April 2010, was written in response to the VCSA's directive. Since then, CIO/G-6 has crafted the *Guidance for 'End State' Army Enterprise Network Architecture* version 2.0 to provide direction for the entire Army Enterprise Network. The *Common Operating Environment (COE) Architecture* is a key part of the broader enterprise network architecture.

The Army Enterprise Network enables full-spectrum operations through all phases of training and deployment. The COE is an approved set of computing technologies and standards that will enable secure and interoperable applications to be developed rapidly and executed across a variety of computing environments: server, client, mobile devices, sensors and platforms. This document:

- defines the COE and computing environments;
- describes the computing environments' architecture and services;
- specifies COE principles and the minimum technical architecture standards targeted for the Operating Force in the FY 13-14 timeframe; and
- details a maturity model that will be used to conduct cost-benefit trades and to evaluate programs' alignment with the COE goals for Program Objective Memorandum 13-17.

Properly executed, implementation of this architecture will enable the Army to develop, test, certify and deploy software capabilities more quickly. The next step is for the Assistant Secretary of the Army (Acquisition, Logistics and Technology) to develop the COE Implementation Plan, which will identify the implementation strategy, time lines, effective dates and key milestones for moving Army systems to the COE.

Approved:

10/4/2010

LTG Jeffrey A. Sorenson
United States Army | Chief Information Officer/G-6
Pentagon, Washington, DC 20310

Table of Contents

1.0 Introduction 4
1.1 Background 4
1.2 Approach 5
1.3 Purpose 7
2.0 Common Operating Environment/Computing Environment 7
2.1 Definition 7
2.2 Principles 9
3.0 Mission Environments 10
4.0 Control Points 11
5.0 Computing Environments – Technical Configuration 19
5.1 Enterprise and Tactical Server Computing Environment 20
5.2 Client, Sensors, Mobile and Platform Computing Environments 22
5.2.1 Standard Applications 23
5.2.2 Application Part Library 23
5.2.3 Security Configuration 23
5.2.4 Operating System 24
5.2.5 Hardware 24
6.0 Program Maturity Model 24
6.1 'As Is' Maturity Assessment Process 25
6.2 'As Planned' Maturity Assessment Process 26
7.0 Way Ahead 26
TAB 1: Enterprise/Tactical Server Standards 28
TAB 2: Client (Tactical) Standards 43
TAB 3: Platform Standards 46
TAB 4: Mobile Standards 51
TAB 5: Sensor Standards 53
TAB 6: Program Maturity Model Criteria 56

Development Attributes 56
Deployment Attributes 60
TAB 7: Acronyms 63

Appendix C: Common Operating Environment Architecture

1.0 Introduction

On 28 December 2009, the Vice Chief of Staff of the Army (VCSA) directed CIO/G-6 to develop 'as is' and 'end state' network architectures to guide network development, procurement and enhancement. The *Army Network Architecture Strategy – Tactical* version 1.1, dated 6 April 2010, was crafted in response to the VCSA's memorandum. Since then, CIO/G-6 has written the *Guidance for 'End State' Army Enterprise Network Architecture* version 2.0 to provide direction for the entire Army Enterprise Network. The *Common Operating Environment (COE) Architecture* is a key component of that guidance. The COE will be validated and republished twice each year at a minimum.

1.1 Background

The current Army approach to information technology implementation and management is cumbersome and inadequate to keep up with the pace of change. The acquisition process focuses on the development and fielding of systems by programs that were established to deliver capability for a specific combat or business function. Based on functional proponent requirements, program managers individually choose and field hardware platforms and software infrastructures. Meanwhile, to support ongoing conflicts, Army and combatant commanders independently procure commercially available solutions, often installing and customizing them in theater. As a result, deploying and deployed units frequently must plan and execute operations using multiple computer systems with different hardware, operating systems, databases, security configurations and end-user devices.

The extraordinary scale and scope of this complex integration raise cost, decrease interoperability, increase network security risk, expand the deployment footprint and add a tremendous burden to managing configurations. Most importantly, the process carries significant operational impacts.

The intent of the COE architecture is to normalize the computing environment and achieve a balance between unconstrained innovation and standardization. In the commercial sector, computing environments have become commodities and applications are developed and delivered on commoditized and inexpensive systems (for example, the Apple iPhone and Google Android mobile devices). With a COE, the Army can establish a framework similar to industry best practices. Communities of interest will be able to:

produce high-quality applications quickly and cheaply; improve security and the defense posture; reduce the complexities of configuration and support; and streamline and facilitate training. This is a wholesale shift from the Army's traditional procurement of systems with dedicated software and hardware. Instead, applications will be designed, developed and deployed on a common computing environment, allowing the end user to download what he needs when he needs it.

1.2 Approach

The Army Enterprise Network, illustrated in Figure C1, is comprised of four networks: the Global Defense Network, the At Home/TDY Network, the At Post/Camp/Station Network and the Deployed Tactical Network. The Army Enterprise Network enables full-spectrum operations through all phases of deployment. The COE enables secure, uniform and interoperable access to warfighter capabilities across the Army enterprise.

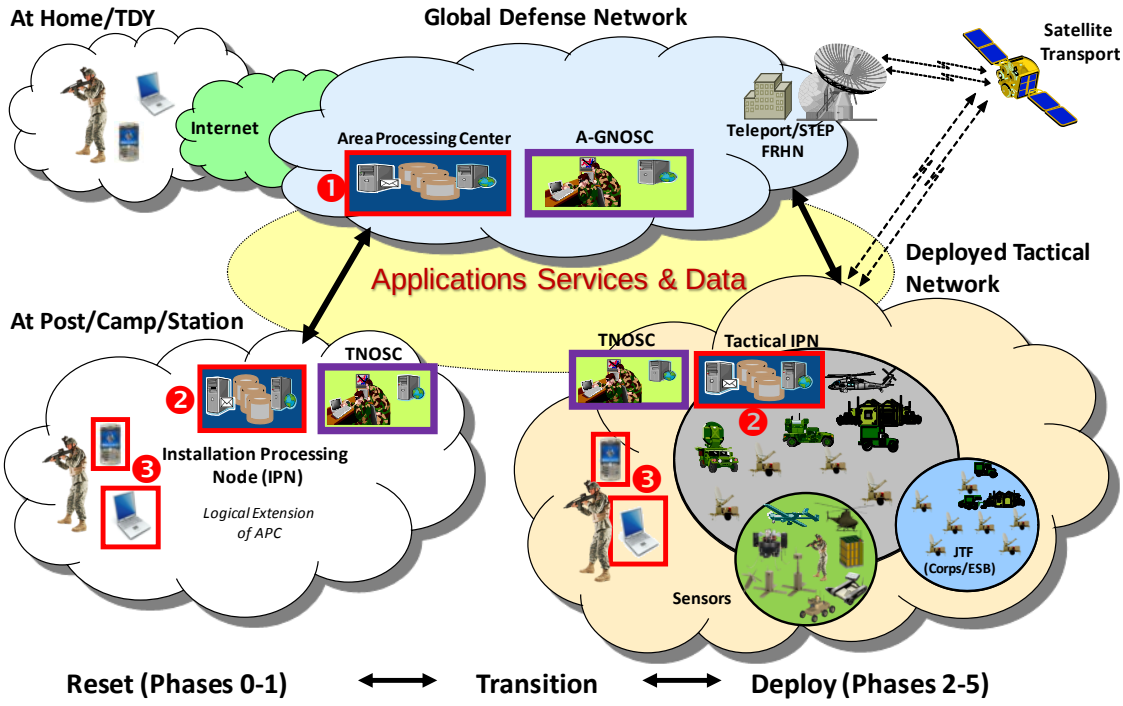

Figure C1 - Army Enterprise Network (LandWarNet)

Experience shows that conformance to standards leads to optimization. This document targets the FY13-17 Program Objective Memorandum period, providing standards for computing environments that execute within the Common Operating Environment

framework. It applies to all organizations and agencies of the Army, U.S. Army Reserve and Army National Guard (to include standalone Reserve Centers located in the continental United States and U.S. territories and possessions). The scope of the COE architecture is limited to programs that support the operating force across full-spectrum operations and through all phases of training and deployment, as depicted by the highlighted red boxes in Figure C1. The COE architecture does not contain a comprehensive, rigid set of instructions for developing applications or systems. It also does not currently apply to embedded, real-time or safety-critical vetronics and avionics systems. Guidance for these systems will be provided in the next update to the COE Architecture Appendix.

The following items are included in this document's scope.

❶ **Area Processing Centers in the Global Defense Network:** In support of the Federal Data Center Consolidation Initiative, the Army is consolidating data centers into Area Processing Centers (APCs). APCs deliver enterprise services on an area and theater basis from a limited number of standardized, centrally managed facilities connected to the Defense Department's global high-speed backbone network. APCs also host functional applications (e.g., Battle Command Common Services (BCCS), business, intelligence) for use by operating and generating forces. APCs not only centralize Army, Joint and coalition data, applications and services, but also support a worldwide DoD intranet by which a single connection allows a user to access these resources from anywhere, at any time, in any operational environment.

❷ **Tactical Installation Processing Nodes (IPN):** Forward-deployed forces are provisioned instances of high-performance computing, storage or enterprise services in order to meet mission-specific performance requirements. BCCS is currently designated as the Tactical IPN. It enables host capabilities for SharePoint and web development in a service-oriented infrastructure[1]. Additionally, the Battle Command Server provides interoperability services, including Publish and Subscribe Services and the Data Dissemination Service. The server also supports convergence with the U.S. Marine Corps by providing a data exchange gateway that allows the direct exchange of Common Operating Picture data.

---

[1] SharePoint, Active Directory and Exchange are available via Microsoft Enterprise License Agreement II (MS ELA II), W91QUZ-09-A-0004, awarded 30 June 2009. AR 25-1, Para. 6-2e governs the use of the products on this ELA.

❸ **End-User IT Devices for Operational Forces:** Tactical and non-tactical end-user IT devices include mobile devices and client computers.

1.3 Purpose

The purpose of this document is to provide guidance to program managers and solution developers to help them maximize scarce resources for the benefit of the Army Enterprise. Establishing a COE will enable approved Army applications, services and data to achieve the following characteristics.

- Available anywhere on the network to authorized users from any suitable Army-managed device.
- User security and configuration are remotely administered and available wherever user connects.
- Reduced complexity and risk through standardized computing environments.
- Common standards that ensure mission-critical computing environments are recoverable, flexible, and backward- and forward-compatible across the Army/DoD network in alignment with continuity of operations.
- Reduced C4/IT logistics footprint, which decreases management burden and increases mobility, by leveraging Army assets across programs (servers, etc.).
- Efficient and effective interoperability with mission partners achieved through the use of tested and certified common components.

2.0 Common Operating Environment/Computing Environment

2.1 Definition

The COE illustrated in Figure C2 is an approved set of computing technologies and standards that enable secure and interoperable applications to be developed and executed rapidly across a variety of computing environments (i.e., server(s), client, mobile, sensors and platform). Each computing environment has a minimum standard configuration that supports the Army's ability to produce and deploy quickly high-quality applications, and to reduce the complexities of configuration, support and training associated with the computing environment.

Figure C2 - Common Operating Environment

The characteristics of each computing environment are detailed below.

- ***Enterprise Server*** **–** high-bandwidth network, server-class computing and environmental support capable of operating enterprise-scale applications and data center services.

- ***Tactical Server and Client*** **–** transportable server-class hardware paired with powerful client workstations connected by a generally reliable network with moderate to high bandwidth located in command posts or improved building environments. The tactical server and client computing environments allow command post mission environment users and systems to leverage capabilities offered by the enterprise, as well as to operate robust capabilities locally.

- ***Platform (ground and air)*** **–** reduced network, computing and environmental contexts (size, weight and power); requires tailoring and flexibility to accommodate smaller form-factors and limited bandwidth.

- ***Mobile*** **–** small handheld devices (i.e., Smartphone, slate) and technologies for the mobile computing environment, often based on lightweight commercial-off-the-shelf technology.

- ***Sensors*** **–** specialized, human-controlled or unattended computing environments. Sensors are organized by family (e.g., material detection, video surveillance, task robot) with different characteristics and capabilities based on mission requirements.

2.2 Principles

The principles are guiding statements that communicate fundamental elements, rules and qualities necessary for the Army to realize its desired application characteristics. The principles reflect the collective direction sought for Army applications and should be used in conjunction with the Program Maturity Model (Section 6.0) to direct decision making about technologies in the COE. The objective is for application programs to abide by these principles during the target timeframe. Migration of programs to these principles will be detailed in the ASA(ALT) Implementation Plan.

- The COE is standards-based. Applications and application components will adhere to Army/DoD standard naming conventions, reside in common libraries and be deployed using standard release-management processes.

- The COE will use DoD- and Army-mandated applications and standards. To increase integration, enterprise-selected applications and standards will be the default.[2] The COE will leverage DoD- and Army-mandated products to the maximum extent possible. Details will be provided in the COE Implementation Plan.

- The COE must be scalable across the enterprise. Applications will be developed for the server environment and extended to the tactical level unless mission requirements demand otherwise. Use of the server environment means fewer server instantiations, thus making applications easier to update, to operate and to maintain. Server-side applications will be accessed by the customer through a client computer or a handheld device via a standards-based web browser. For example, to improve our defense posture, the number of Cross-Domain Solutions (CDS) will be minimized. CDS will be hosted at an enterprise server location unless unique validated mission requirements demand that they be hosted in the local strategic or tactical environment.
- The COE defaults to COTS solutions. The COE will leverage commercial-off-the-shelf (COTS) solutions and other commercial capabilities first, including open

[2] Examples of enterprise applications include Sharepoint, Active Directory and Exchange. Use of enterprise applications is mandated by a joint memorandum from the CIO/G-6 and the Assistant Secretary of the Army (Acquisition, Logistics and Technology), subject "Use of Computer Hardware, Enterprise Software and Solutions (CHESS) as the Primary Source for Procuring Commercial Information Technology (IT) Hardware and Software", dated 4 May 2009; and AR 25-1, Para. 6-2e.

source solutions. The objective is to leverage market-leading COTS technologies to the fullest extent possible and to utilize DoD solutions for military-specific needs. Customization of packaged applications will be minimized. Reuse of existing packages will be exploited where possible.

- The COE must remain relevant. Emerging commercial technologies will be continually assessed for inclusion in the COE. Similarly, current technologies will be continually assessed for obsolescence; those that are obsolete and/or no longer relevant will be retired (i.e., sunsetting). All computing environments and the components that execute in the computing environment will stay current (within two years of version release). Software used in the field will be limited to versions maintained by the software vendor.

- The COE is hardware agnostic. The COE is independent of any hardware solutions; hardware must be suitable to meet COE and software performance requirements.

- The COE will be interoperable and compliant with overarching directives. A common data vocabulary and schema designed to facilitate data sharing will be aligned with DoD directives.

3.0 Mission Environments

The mission environments in which Soldiers operate (Figure C3) are differentiated by varying network bandwidth requirements (latency, high bit-error rate), SWaP (size, weight and power), environmental factors and location permanence. Each mission environment is supported by a limited number of standardized computing environments that provide needed capability and integration with other computing environments.

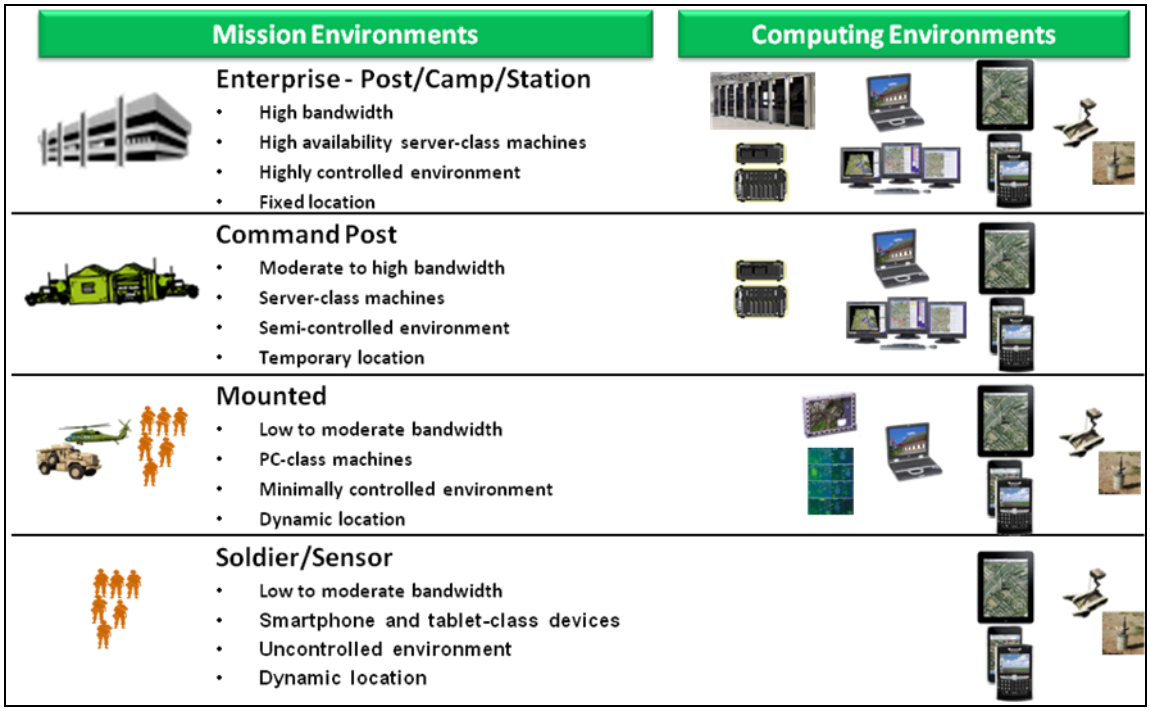

Figure C3 - Mission Environments Mapped to Computing Environments

4.0 Control Points

Seamless integration must exist across the Army Enterprise Network and between computing environments. Control points facilitate the integration of mission environments (Figure C4 and Table C1), and serve as intermediaries between mission environments and the corresponding computing environments. Control points also isolate (or firewall) local standards from the rest of the enterprise.

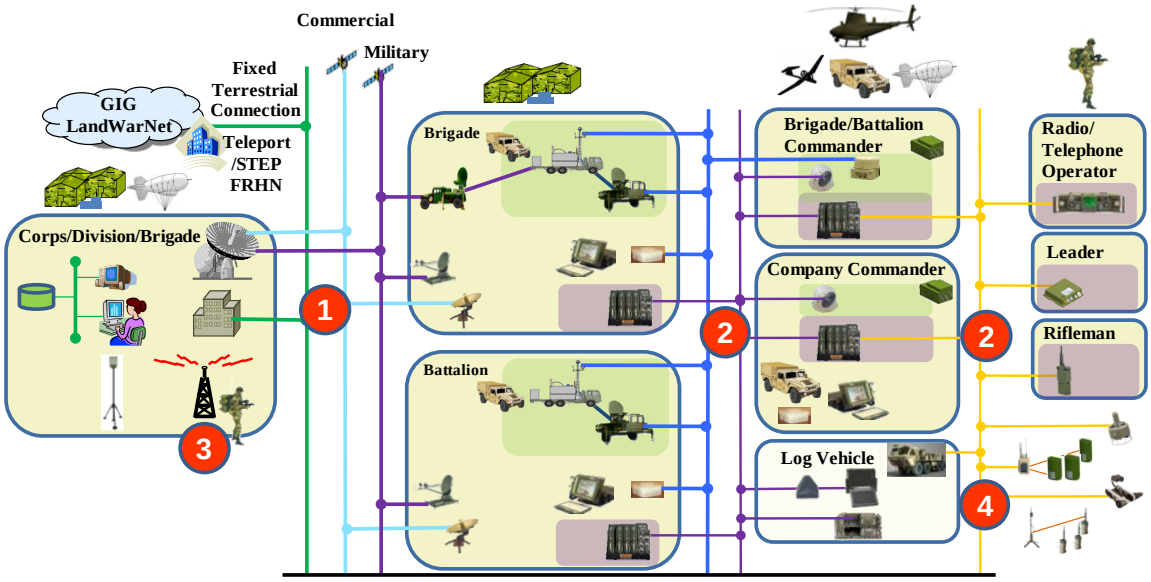

Figure C4 - Tactical Network and Control Points

Control points are placed throughout the architecture to enable and to enforce the following requirements.

- Interoperability – Logical boundary of mission environments at which software/systems exchange of useful data is critical to the Army and the Joint enterprise.
    - Structured Data – Data that are defined by a data model and are easily retrieved by a program or user (e.g., databases, geospatial data, spreadsheets)
    - Unstructured Data – Data that have no defined data model (e.g., documents, presentations, pictures, audio, video) and are not easily processed for analyses by computers
- Security – Logical boundary within the enterprise architecture where access to data, services and software must be controlled.
- Gateways – Act as an intermediary for requests from one computing device to another. A gateway evaluates the request according to its filtering rules (e.g., by IP address or protocol).

Interoperability, security and gateway solutions that exchange information across control points will be configured to optimize network performance and minimize bandwidth use.

Control Point ❶ – Enterprise to TOC/Command Post: Information is flowing between a fixed, highly secure location with a terrestrial network connection and a temporary location (at the halt) over SATCOM. This provides a control point for access between Army tactical forces and the Army Enterprise, and for interface with COCOMs, mission partners and the Joint enterprise.

- Interoperability – Exchange of data and information at this boundary is critical to the command post's ability to interact with the Army Enterprise. These interoperability network standards also will apply to commanders' platforms that have additional network capacity and mission-command systems. Standards include but are not limited to:
    - Authentication – PKI or Active Directory
    - Web Service Authorization – TS3
    - Service Discovery – UDDI
    - Synchronous Collaboration – H.323 / H.264

    Structured Data

    - Message exchange – SOAP and REST/XML (aligned with commercial and DoD standards)
    - Publish/Subscribe Service – XML (DDMS/DDS) (aligned with commercial and DoD standards)
    - Database – ODBC
    - Geospatial data – KML/MIL-STD 2525C

    Unstructured Data

    - Email – Exchange/SMTP/IMAP4/MAPI
    - Chat – XMPP
    - Portal – SharePoint
    - VoIP – AS-SIP
- Security – Access control must prohibit unauthorized access from the enterprise to the TOC and vice-versa. Standards will include:
    - network access control – firewall (802.1X);
    - external access control – firewall/IDS

- encryption– NSA/NIST-certified solutions
- Key Management - EKMS/KMI-compliant solutions
- cross-domain access/guards – CDS/guard solutions;
- certificate validation – OCSP;
- end-point protection – Host-Based Security System (HBSS)[3]
- enterprise service management – Remedy/ITSM, IP Management/SPECTRUM (configured to roll up data at control points); and
- patch management – remote: SCCM, WSUS and CA Unicenter.

- Gateways – The enterprise/command post server is responsible for translation to/from mission-partner data standards and moving this data between security domains.
    - Data Mediation Standards: DDS/XML (aligned with commercial and DoD standards) to mission-partner exchange method

Control Point ❷ – Enterprise/Command Post to Platform/Soldier/Sensor: Information is flowing between a fixed, somewhat stable network at the command post to individual platforms, Soldiers or sensors, typically over a disadvantaged network link. This provides a control point for interface to/from the enterprise standard/protocol to a local standard/protocol that is more optimized for disadvantaged networks.

- Interoperability – Authentication via PKI, LDAP or Active Directory. Exchange of data between the TOC and the platform/Soldier/sensor is critical to the commander's ability to operate. The prescribed interface is C2 Messaging – VMF. Geospatial data standard is VMF/MIL-STD 2525C.
- Security – Access control must prohibit unauthorized access from the enterprise to the platform/Soldier/sensor and vice-versa. No additional cross-domain platform, Soldier or sensor solutions will be permitted and those in existence will be evaluated for convergence. Standards will include:
    - network access control – local, varies;
    - external access control – network gateway;

[3] DoD-approved HBSS products are specified in a classified OPORD issued by JTF-GNO and in FRAGOs.

- encryption– NSA/NIST-certified solutions;
- key management - EKMS/KMI-compliant solutions;
- end-point protection – Host-Based Security System (HBSS);
- enterprise service management – Remedy/ITSM, IP Management/SPECTRUM (configured to roll up data at control points); and
- patch management – manual.

- Gateways – The enterprise/command post server is responsible for translation of XML/SOAP to/from VMF.

Control Point ❸ – Enterprise/Command Post to Soldier: Information is flowing between a fixed, somewhat stable network at the command post to individual Soldiers at a point where the network supports commercial protocols.

- Interoperability – Exchange of data between command post and Soldier is critical to the collection of relevant, real-time information. Efficient commercial protocols will be used. Standards include:
  - authentication – Active Directory or PKI;
  - web service authorization – TS3;
  - service discovery – UDDI; and
  - synchronous collaboration – H.323/H.264.

  Structured Data

  - Message exchange – SOAP and REST/XML (aligned with commercial and DoD standards)
  - Publish/subscribe service – XML (DDMS/DDS) (aligned with commercial and DoD standards)
  - Database – ODBC
  - Geospatial data – KML/MIL-STD 2525C (Refer to Tab I to this Appendix I, *Geospatial Enterprise Network Guidance*, for a detailed use case of one functional organization's management of structured data)

  Unstructured Data

  - Email – SMTP
  - Chat – XMPP

    - Portal – SharePoint
    - VoIP – AS-SIP
- Security – Access control must prohibit unauthorized access from the TOC to the Soldier and vice-versa. No additional cross-domain Soldier solutions will be permitted and those in existence will be evaluated for convergence. Standards will include:
    - network access control – firewall (802.1X);
    - external access control – network gateway; and
    - patch management – remote: SCCM, WSUS and CA Unicenter.
- Gateways – Email translation will be done by the enterprise/command post server for email (Exchange/SMTP/IMAP4/MAPI).

	Control Point 1 Enterprise - P/C/S to Command Post	Control Point 2 Enterprise/Command Post to Platform/Soldier/Sensor	Control Point 3 Enterprise/Command Post to Soldier	Control Point 4 Platform/Soldier to Sensor
Interoperability*				
Authentication mechanism	PKI or Active Directory	PKI, Active Directory or LDAP	PKI or Active Directory	PKI (Local Repository)
Web service authorization	TS3	X	TS3	X
Service discovery	UDDI	X	UDDI	X
Synchronous collaboration	H.323 / H.264	X	H.323 / H.264	X
Structured Data				
Message exchange	XML (SOAP/REST)	VMF	XML (SOAP/REST)	VMF
Pub/sub-service	XML (DDMS/DDS)	X	XML (DDMS/DDS)	X
Database	ODBC	X	ODBC	X
Geospatial data	KML/MIL-STD 2525C	VMF/MIL-STD 2525C	KML/MIL-STD 2525C	VMF/MIL-STD 2525C
Unstructured Data				
Email	Exchange SMTP/IMAP4/MAPI	X	Exchange/SMTP/IMAP4/MAPI	X
Chat	XMPP	X	XMPP	X
Portal	Sharepoint	X	Sharepoint	X
VoIP	AS-SIP	X	AS-SIP	X
Security				
Network access control	802.1X	Local, varies	802.1X	Local, varies
External access control	Firewall/IDS	Network Gateway	Network Gateway	Network Gateway
Cross-domain access/guards	CDS/Guard solutions	X	X	X
Certificate validation	OCSP	X	X	X
End-point protection	Host-Based Security System (HBSS)	Host-Based Security System (HBSS)	X	X
Enterprise service management	Remedy/ITSM, IP Management/SPECTRUM**	Remedy/ITSM, IP Management/SPECTRUM**	X	X
Patch management	Remote: SCCM, WSUS and CA Unicenter	Manual	Remote: SCCM, WSUS and CA Unicenter	Manual
Gateways				
Data Mediation Standards	Army to/from mission partners	X	X	X
Message Exchange	X	XML Translation/VMF	X	X
Email Exchange	X	X	Exchange/SMTP/IMAP4/MAPI	X

X - Not Supported

* For control point 1 the interoperability network standards also will apply to commanders' platforms that have additional network capacity and C2 systems.

** Tools configured to roll up data at control points.

Table C1: Control Points

Control Point ❹ – Platform/Soldier to Sensor: Information is flowing between a platform/Soldier and a sensor, both of which can be on the move.

- Interoperability – Authentication via PKI or Active Directory. Exchange of data between platforms and the Soldier/sensor is critical to the collection of relevant, real-time information. Network protocols that are efficient will be the standard. The prescribed interface is Mission Command Messaging – VMF. The geospatial data standard is VMF/MIL-STD 2525C.
- Security – Access control must prohibit unauthorized access from the platform/Soldier to the sensor and vice-versa. No additional cross-domain Soldier or

sensor solutions will be permitted and those in existence will be evaluated for convergence. Standards will include:

  - network access control – local, varies;
  - external access control – network gateway; and
  - patch management – manual.

- Gateways – No translation required.

In the future, the Army must balance oversight, testing and certification against agile and responsive capability development. Control points will be central to streamlining the certification and accreditation process. Currently, the Army conducts interoperability testing according to the mission thread approach. This method assesses interoperability by directly testing each system against every other system with which it might interact across today's 86 mission threads. Mission threads represent operational requirements and are designed to quantify a system's response to a series of select scenario events. Testing of these mission threads can take several months and requires that every system in the testing chain be present and operable.

Instead of this time-consuming and cumbersome process, the Army intends to utilize an interface-based testing approach (see Figure C5). This technique establishes a validated test bed, known as the reference implementation.

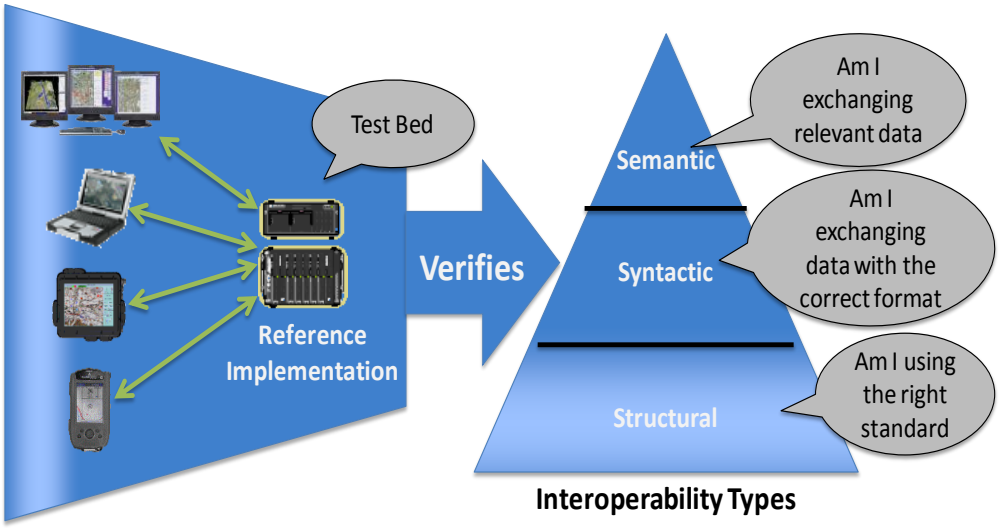

Figure C5: Interface-Based Testing Approach

Each candidate system is then evaluated for interoperability with that test bed. Only when the system's critical interfaces exhibit the required syntactic and semantic

interoperability – that is, data are exchanged in the correct format and consistently interpreted accurately -- at the specified control points against the test bed will the system earn certification. This significantly simplified procedure will greatly speed accreditation and certification, thus reducing test costs and greatly accelerating the fielding of new technology. This is essential in today's operating environment.

Testing of COE control point interoperability will be based on the results of the Interface-Based Testing Pilot completed in August 2010. The detailed test plan and supporting implementation approach for control point interfaces will be provided to ASA(ALT) by December 2010.

5.0 Computing Environments – Technical Configuration

Each computing environment has a minimum standard configuration that supports quick production and deployment of high-quality applications, and reduction in the complexities of configuration, support and training associated with the computing environment.

5.1 Enterprise and Tactical Server Computing Environment

The enterprise and tactical server computing environments (illustrated in C6) comply with DISA's Joint C2 Architecture[4]. They consist of the items within the red box: C2 infrastructure services, enterprise services (including those locally hosted for the tactical computing environment) and the data cloud.

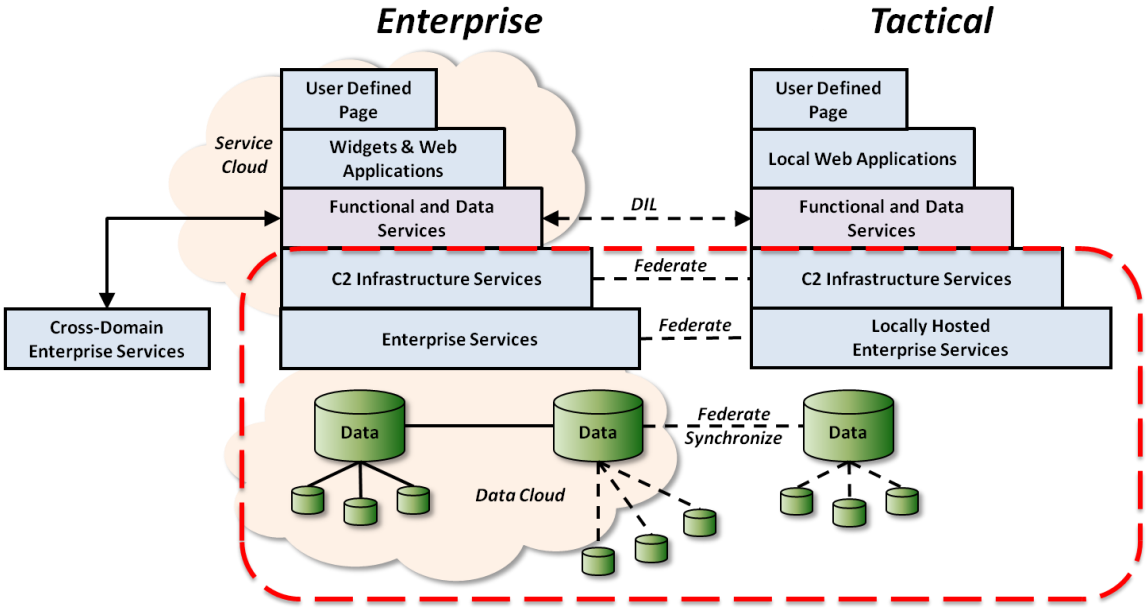

Figure C6 - Enterprise and Tactical Server Computing Environments

[4] https://www.us.army.mil/suite/portal/index.jsp

Key services provided by enterprise and tactical servers are detailed in Table C2.

Table C2 - Server Computing Environment Services		
Enterprise Services	**Enterprise**	**Tactical**
Security Services: Public Key Infrastructure (PKI), Robust Certificate Validation Services (RCVS), Attribute Service	✓	+/-
Machine to Machine (M2M) Messaging	✓	✓
Metadata Registry	✓	+/-
Service Discovery	✓	+/-
Content Discovery Enterprise Search	✓	
Collaboration: Bulletin/Discussion Board (e.g., SkiWeb)	✓	+/-
Collaboration: Chat (e.g., Jabber)	✓	+/-
Collaboration: Web Conferencing (e.g., Defense Connect On-line (DCO))	✓	✓
Enterprise Service Management	✓	+/-
GIG Content Discovery Service (GCDS)	✓	
Social Networking	✓	
Mediation	✓	✓
Geospatial Visualization – Enterprise Services (GV-ES)	✓	✓
Widget Framework	✓	+/-
Security Services: Online Certificate Status Protocol (OCSP), Local Attribute Service	✓	✓
Content Discovery Federated Search		✓
Collaboration: Cross-Domain Collaborative Information Environment (CDCIE), Chat		✓
C2 Infrastructure Services	**Enterprise**	**Tactical**
User Support	✓	✓
Training	✓	✓
Workflow Engine	✓	✓
Redirection	✓	✓

✓Available at the enterprise level.
+/- Federated from locally hosted enterprise services. Provides for disconnected operations.

The computing environment standards for enterprise and tactical servers are detailed in TAB 1.

5.2 Client, Sensors, Mobile and Platform Computing Environments

The client, sensors, mobile and platform computing environments (illustrated in C7) each consist of standard applications, an application parts library, a security configuration and an operating system.

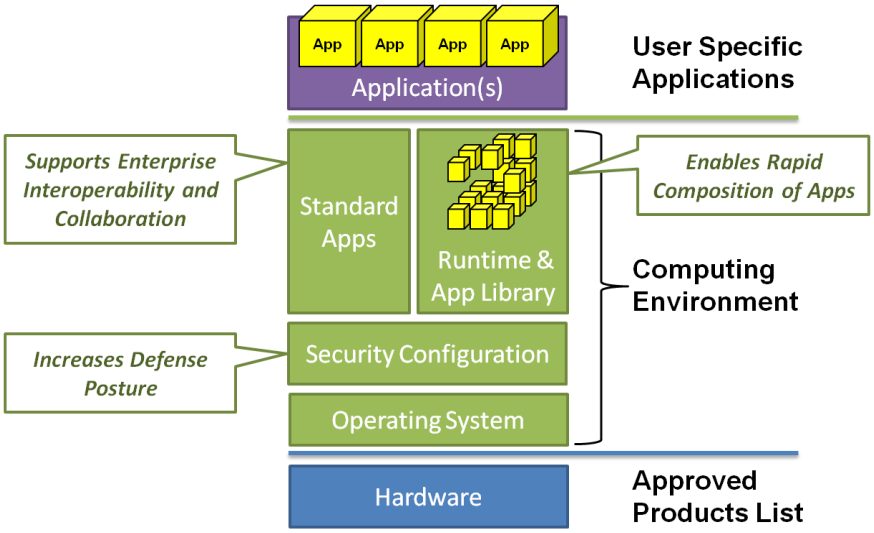

Figure C7 - Client, Sensors, Mobile and Platform Computing Environments

Each standard computing environment supports the Army's need to develop applications in a more consistent, agile, effective and efficient manner. Computing environments remain uniform regardless of the network's hardware or the user-specific applications in that computing environment. Using the Army Golden Master (AGM) construct, a standard image will be managed for each computing environment's operating system. One baseline of each standard image will be released per year, with cumulative updates that include security setting changes, patches, information assurance and vulnerability assessments, application updates and utilities updates. Standard image releases will be automated by utilizing the Security Control Compliance Matrix, Windows Server Update Services and CA Unicenter. The associated standards that define the minimum configuration required to produce and deploy rapidly secure, interoperable, high-quality applications that run as intended are defined in TABs 2-5. Identifying the minimum set of standards allows the Army to maintain agility; defining granular standards and locking down computing environments would sacrifice this essential characteristic. Standards are organized by the building blocks of the computing environments shown in Figure C7. A description of each building block follows.

5.2.1 Standard Applications

A fixed set of applications is included in the standard image to support enterprise interoperability and collaboration, while other applications are selected by users based on mission requirements. Standard applications are typically procured using enterprise licenses and include:

- email client;
- chat client;
- browser;
- document viewer;
- document editor;
- presentation editor; and
- VPN client (SSL).

5.2.2 Application Part Library

The Application Part Library contains the application runtime engines and reusable component libraries that are used by applications. These are preloaded on the system to reduce the size of the installation effort. Additionally, these components, reusable code and data standards, and dictionaries are available in the development environment to help the developer build new applications and functionality. Reuse of previously tested and certified components will reduce test and certification time and facilitate rapid releases. The Application Part Library includes:

- approved runtime engines and
- component library/registry.

5.2.3 Security Configuration

The standard security configuration efficiently and consistently hardens systems connected to the Army network by reducing their attack surface. The security configuration is aligned with DoD security directives and the level of risk the Army is willing to accept. The security configuration includes software and processes that comply with the Federal Desktop Core Configuration(FDCC), an Office of Management and Budget mandate that requires all Federal agencies to standardize configuration in order to strengthen Federal IT security. The security standards include:

- anti-virus;
- standard Army security policy (aligned with FDCC);

- patch management; and
- identity management.

5.2.4 Operating System

The operating system (OS) is an Army-approved commercial OS that manages computer hardware and provides common services.

5.2.5 Hardware

Hardware is selected from an approved products list that is designed to standardize infrastructure and to ensure compatibility.

6.0 Program Maturity Model

The intent of the Maturity Model is to depict the strategic goals of the COE and to identify incremental steps in obtaining these goals. Additionally, the Maturity Model will be used to conduct cost-benefit analysis prior to investments. The Maturity Model is comprised of 10 attributes selected for their relevance to achieving the Army's goal of developing and deploying applications in an agile, efficient and standard manner. The attributes are grouped into two major categories: development and deployment (as shown in Table C3). Development attributes assess the relative maturity of the program's development standards, processes, tools, software reuse and IA. Deployment attributes assess the relative maturity of the program's coupling (the degree to which components depend on each other), organizational reach, information architecture and presence. Each attribute has well-defined criteria for attaining increasing levels of maturity on a scale of one to four. The goal is not for each and every program to achieve Level 4 maturity, but rather to understand the current maturity level and to determine whether investment is warranted to move up the maturity scale. The Maturity Model will be used to measure the baseline and plans against a set of goals to determine each program's 'as is' and 'as planned' maturity levels.

Development Attributes	Level 1	Level 2	Level 3	Level 4
Architecture Standardization	No standards	Local standardization Joint /Coalition	Army standardization	Joint/Coalition standardization
Development Process	Developer-defined process	Local standards and procedures	Army-defined process	Joint/Coalition-defined process
SDK/IDE Scope of use	A system	Family of systems	DoD programs of record (PORs)	Industry, Army employees, DoD programs
Component Reuse	No specific support	Code reuse	Component sharing	C&A-validated secure components
Information Assurance (IA)	Security not considered	Security added post development	Security included in system design	Security conforms to all DoD standards
Deployment Attributes	**Level 1**	**Level 2**	**Level 3**	**Level 4**
System Coupling	Hardware & software (non-AGM)	Hardware & software (with AGM)	Co-host with other software	Application delivered from Market Place
Organizational Reach	Functional level	Enterprise level	Joint	Joint and Coalition
Availability of Capability and Data	System	LAN	Army / LandWarNet	Anywhere on DoD network
Information Sharing Coupling	Duplicative of authoritative data sources	Duplicates but synchronizes with authoritative data sources	Caches and synchronizes with authoritative data sources	Maximum use when needed with authoritative data sources
Presence and Sustainment	No resources / funding	Support requirements funded as needed	Funding in place. Regular system upkeep performed	Support funded. Viability and penetration tracked.

Table C3 - Model (see TAB 6 for additional details)

6.1 'As Is' Maturity Assessment Process

During the 'as is' maturity assessment process, a program is evaluated against the four maturity levels' criteria for each attribute in the model. The maturity rating assigned to each attribute is the one that most closely maps the maturity model's criteria to the characteristics observed in the specific software technology being assessed. A program must meet or exceed all the criteria described in the attribute's level definition to be assessed at that level of maturity. An overall maturity rating is determined by averaging

the maturity ratings for each attribute. All criteria are equally weighted. In many cases a program's overall maturity rating may fall between levels (e.g., overall maturity rating of 1.7).

6.2 'As Planned' Maturity Assessment Process

The 'as planned' maturity assessment is executed using the same process as the 'as is' but also considers cost. When ascending from one level to the next, if the cost delta between levels is higher in relative terms than the prior investment, a cost-benefit analysis must be done in coordination with the DA Staff and ASA(ALT) to confirm that the investment is worth the added maturity level.

7.0 Way Ahead

Properly executed, implementation of this architecture will enable the Army to develop and deploy applications more rapidly. CIO/G-6, in conjuction with ASA(ALT) and G-8, will assess current and planned technical maturity levels of designated acquisition programs prior to Weapons Systems Reviews. The next step is for ASA(ALT) to develop a COE Implementation Plan that describes the steps and schedule for moving tactical Army systems to the COE. Roles and responsibilities for the COE Implementation Plan are portrayed in Table C4. The plan will inform the FY13-17 weapon systems reviews and subsequent FY13-17 Program Objective Memorandum investments. Program Executive Officers and separately reporting Program Managers must comply with the guidelines in this appendix and the ASA(ALT) Implementation Plan in order to obtain FY13-17 POM funding for the development and acquisition of IT devices and systems and National Security Systems.

		RESPONSIBLE ORGANIZATION(S)				
		ASA(ALT)	G6	G8	PMs/PEOs	Others
TASKS	(1) Define technical standards for COE and CEs	Support G6	Lead			
	(2) Determine technology solutions that meet the standards	Lead	Support ASA(ALT)			
	(3) Federate the CEs (i.e., governance of COE)	Lead	Support ASA(ALT)			
	(4) Define governance structure for CEs	Lead	Support ASA(ALT)	Provide resource allocations		SED integrator for platform CE
	(5) Schedule a phased implementation for migrating to the CE.	Lead		Provide cost impacts	Provide schedule and technology impacts	
	(6) Work with S&T community to develop Army-unique solutions as required (e.g., low-bandwidth proxies)	Lead				CERDEC, AMRDEC, ARL technology insertions
	(7) Continually reevaluate commercial standards to ensure relevancy and applicability to CE	Support G6	Lead			
	(8) Re-look emerging COTS technologies to fill gaps and/or replace GOTS technologies (e.g., tactical comms/IA)	Lead	Support ASA(ALT)			CERDEC, AMRDEC, ARL technology insertions
	(9) Define a common COE data model	Support G6	Lead with JFCOM			
	(10) Adjust development focus from infrastructure to applications	Lead	Support	Provide resource allocations	Execute the task	

Table C4 - Implementation Plan Roles & Responsibilities

TAB 1: Enterprise/Tactical Server Standards

The server(s) computing environment consists of enterprise servers running in fixed locations, such as Area Processing Centers (APCs) and tactical servers operating in tactical mission environments (command posts). While many of the standards designed for one server environment will apply to another, significant differences exist.

Enterprise Servers – characterized by high-bandwidth network, computing and environmental support capable of operating enterprise-scale data and application center services. The services and standards for enterprise servers are detailed in TAB 1, Table 1. A detailed list of enterprise server standards mapped to services can be found in Table 1, below.

The table immediately below provides an explanation of the abbreviations used in the standards tables below:

Column	Status Code	Explanation
DoD Information Technology Standards Registry (DISR)	**M**	DISR Standard ID, Standard Title and Status are provided. • **Mandated** Standard (M): Mandated standards provide interoperability and net-centric services across the DoD enterprise. They are the minimum set of essential standards for the acquisition of all DoD systems that produce, use or exchange information.
	E	• **Emerging** Standard (E): Emerging standards may be implemented but shall not be used in lieu of a mandated standard. An emerging standard is expected to be elevated to mandatory status within three years. Use of an emerging standard in a TV-1 requires a waiver and a Technology Insertion Risk Assessment. In general, emerging standards should be placed in the TV-2.
	N	• **Non-DISR Standard (N):** Standard is in development and currently not available in DISR.
Technical Reference Model (TRM) Profile	**(p)**	The TRM Profile is provided, including the type (pre-selected (p) and user-defined (u)) as defined below. • **pre-selected (p):** Standards listed represent a minimum set of standards required to support functionality. Where a pre-selected (p) TRM Standard Profile is chosen, all of the specified standards must be included in the resulting TV-1.
	(u)	• **user-defined (u):** A list of standards from which system developers can select is provided.

Table 1 – Enterprise Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Standard Applications					
Metadata Registry	DDMS	Content Discovery profile (p)	DDMS 2.0	Department of Defense Discovery Metadata Specification (DDMS), Version 2.0, 17 July 2008	M
Dynamic Data Storage	SQL	Database Management Services profile (u)	ISO 23950/NISO Z39.50	Information Retrieval (Z39.50): Application Service Definition and Protocol Specification	M
			ISO/IEC 13249-1:2007	Information Technology - Database Languages - SQL multimedia and application packages - Part 1: Framework, Third Edition, 12 February 2007	M
			ISO/IEC 13249-3:2006	Information Technology - Database Languages - SQL multimedia and application packages - Part 3: Spatial, Third Edition, 26 October 2006	M
			ISO/IEC 9075-1:2003 with Cor. 1:2005 and Cor. 2:2007	Information technology - Database languages - SQL - Part 1: Framework (SQL/Framework), Second Edition, 15 December 2003 with its Technical Corrigendum 1:2005, 15 November 2005 and its Technical Corrigendum 2:2007, 15 April 2007	M
			ISO/IEC 9075-10:2003 with Cor. 2:2007	Information technology - Database languages - SQL - Part 10: Object Language Bindings (SQL/OLB), Second Edition, 15 December 2003 with its Technical Corrigendum 2:2007, 12 April 2007	M
			ISO/IEC 9075-11:2003 with Cor. 2:2007	Information technology - Database languages - SQL - Part 11: Information and Definition Schemas, First Edition, 15 December 2003 with its Technical Corrigendum 2:2007, 12 April 2007	M
			ISO/IEC 9075-2:2003 with Cor. 2:2007	Information technology - Database languages - SQL - Part 2: Foundation (SQL/Foundation), Second Edition, 15 December 2003 with its Technical Corrigendum 2:2007, 12 April 2007	M
			ISO/IEC 9075-3:2003 with Cor. 1:2005	Information technology - Database languages - SQL - Part 3: Call-Level Interface (SQL/CLI), Third Edition, 15 December 2003 with its Technical Corrigendum 1:2005, 25 November 2005	M
			ISO/IEC 9075-4:2003 with Cor. 2:2007	Information technology - Database languages - SQL - Part 4: Persistent Stored Modules (SQL/PSM), Third Edition, 15 December 2003 with its Technical Corrigendum 2:2007, 15 April 2007	M
M2M Messaging	Variable Message Format (VMF)	Military C2 Messages profile	MIL-STD-6017B	Variable Message Format (VMF), June 2009	M

Table 1 – Enterprise Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
		(u)			
Mediation	This is part of DISA Standards-Based Enterprise Services http://www.disa.mil/nces/ (see NCES 101 Briefing Slides for details)	N/A		PM leverages DISA services.	
Collaboration	Web Conferencing (e.g. Army Golden Master: Adobe Connect)	N/A		Army Standard Baseline Configurations for commonly used computing environment within the Army Enterprise Infrastructure.	
	XMPP	Instant Messaging (IM) profile (p)	IETF XMPP	Extensible Messaging and Presence Protocol, December 2004	M
Service Discovery	This is part of DISA Standards-Based Enterprise Services http://www.disa.mil/nces/ (see NCES 101 Briefing Slides for details)	N/A		PM leverages DISA services.	
Publish and Subscribe	• HTTP • UDDI 3.0.2 • SOAP 1.2 • XML 1.0	Web Services	IETF RFC 2616	Hypertext Transfer Protocol - HTTP 1.1, June 1999	M
			UDDI 3.0.2	OASIS Universal Description, Discovery, and Integration Version 3.0.2 UDDI Spec, Dated 2004-Oct-19	M
			W3C SOAP 1.2 Part 1	SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation 27 April 2007	M
			W3C SOAP 1.2 Part 2	SOAP 1.2 Part 2: Adjuncts (Second Edition), W3C Recommendation 27 April 2007	M
			WSDL 1.1	Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001	M
			XML 1.0 (Third Edition)	Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation, 04 February 2004	M
	OMG formal/2007-01-01	Distributed Middleware Object Services	OMG document formal/02-06-01	Common Object Request Broker: Architecture and Specification, Version 3.0, July 2002	M
			OMG formal/2005-01-04	Real Time CORBA Specification, Version 1.2, January 2005	M
			OMG formal/2007-01-01	Data Distribution Service for Real-Time Systems Specification, Version 1.2, January 2007	M
	Data Distribution Service (DDS)	Data Distribution Service		Army standardized publish/subscribe for sending and receiving data service.	
Portal	• Microsoft Office SharePoint Server (MOSS) • JBOSS Enterprise	Portal			N
Service Delivery	Internet Information Server (IIS)/JBOSS	Service Delivery			N

Table 1 – Enterprise Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Enterprise Service Management	This is part of DISA Standards-Based Enterprise Services http://www.disa.mil/nces/ (see NCES 101 Briefing Slides for details)	N/A		PM leverages DISA services.	
Geospatial Foundation	WMS, RPF, Google Earth	Geospatial Web Raster Services Profile p)	WMS 1.3	OpenGIS Web Map Service (WMS) Implementation Specification, 2 August 2004	M
			N/A	RPF/CADRG (Raster Product Format/Compressed ADRG) MILPRF-89038	N
			N/A	Google Earth	N
Geospatial Information	WMS, WMC, KML, and JPEG 2000	Geospatial Web Image Services Profile (p)	WMS 1.3	OpenGIS Web Map Service (WMS) Implementation Specification, 2 August 2004	M
			WMC 1.1	OpenGIS Web Map Context (WMC) Documents Implementation Specification, Version 1.1.0, 19 January 2005	M
			N/A	KML (Keyhole Markup Language) 2.2 – An OGC Best Practice	N
			ISO/IEC 15444-1:2004 | ITU-T Rec. T.800	Information Technology -- JPEG 2000 image coding system: Core coding system	M
			ISO/IEC 15444-9:2005	Information technology -- JPEG 2000 image coding system: Interactivity tools, APIs and protocols, November 17, 2005	M
Geospatial Data	WFS, WCS, NITF, JPEG 2000, and GML	Geospatial Data Profile (u)	WFS 1.1	OpenGIS® Web Feature Service (WFS) Implementation Specification	M
			OGC WCS 1.1.2	Web Coverage Service (WCS) Implementation Standard, Version 1.1.2 (v1.1 Corrigendum 2 release), 2008-03-19	M
			MIL-STD-188-199(1)	Vector Quantization Decompression for the National Imagery Transmission Format Standard, 27 June 1994 with Notice 1, 27 June 1996	M
			MIL-STD-2500C	National Imagery Transmission Format (Version 2.1) for the National Imagery Transmission Format Standard, 01 May 2006	M

Table 1 – Enterprise Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
			NGA STDI-0001 v1.3/CN2	National Support Data Extensions (SDE) (Version 1.3/CN2) for the National Imagery Transmission Format (NITF), 10 July 2007	M
			STDI-0002 v3	The Compendium of Controlled Extensions (CE) for the National Imagery Transmission Format (NITF), v3, 1 August 2007	M
			STDI-0006, 23 July 2008	National Imagery Transmission Format (NITF) Version 2.1 Commercial Dataset Requirements Document (NCDRD), 23 July 2008	M
			ISO/IEC 15444-1:2004 | ITU-T Rec. T.800	Information Technology -- JPEG 2000 image coding system: Core coding system	M
			ISO/IEC 15444-9:2005	Information technology -- JPEG 2000 image coding system: Interactivity tools, APIs and protocols, November 17, 2005	M
			GML 3.1.1	OpenGIS Geography Markup Language Encoding Specification, 7 February 2004	M
Security Configuration					
Security Services	ITU-T X.509	Implement NSA or NIST Public Key Cryptography profile (u)	FIPS Pub 197	Advanced Encryption Standard (AES), 26 November 2001	M
			IETF RFC 2560	IETF Public Key Infrastructure X.509 (PKIX) Online Certificate Status Protocol (OCSP), RFC 2560, June 1999	M
			IETF RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999	M
			IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	M
			ITU-T X.509:2005	Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, August 2005	M
			PKIKMITKNPP	Public Key Infrastructure and Key Management Infrastructure Token (Medium Robustness) PP	M
	WS-Security	Web Services Security (WS Security) profile (p)	IETF RFC 4346	The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006	M
			IETF RFC 4347	Datagram Transport Layer Security, April 2006	M
			SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	M

Table 1 – Enterprise Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
			WS-Security 1.1	Web Services Security v1.1, February 2006	M
Geospatial Foundation	• WMS • RPF	Geospatial Web Raster Services profile (p)	WMS 1.3	OpenGIS Web Map Service (WMS) Implementation Specification, Version 1.3, 15 March 2006	M
				RPF/CADRG (Raster Product Format/Compressed ADRG) MILPRF-89038	
	Google Earth	N/A		Google Earth	
Geospatial Information	• WMS • WMC • KML • JPEG 2000	Geospatial Web Image Services profile (p)	ISO/IEC 15444-1:2004 | ITU-T Rec. T.800	Information Technology -- JPEG 2000 image coding system: Core coding system	M
			ISO/IEC 15444-9:2005 w/Cor 1:2007, Cor 2:2008, Amd 1:2006	Information technology -- JPEG 2000 image coding system: Interactivity tools, APIs and protocols, November 17, 2005 with Cor 1:2007, Cor 2:2008, Amd 1:2006, Amd 2:2008, and Amd 3:2008	M
			WMC 1.1	OpenGIS Web Map Context (WMC) Documents Implementation Specification, Version 1.1.0, 19 January 2005	M
			WMS 1.3	OpenGIS Web Map Service (WMS) Implementation Specification, Version 1.3, 15 March 2006	M
				KML (Keyhole Markup Language) 2.2 – An OGC Best Practice	
Geospatial Data	• WGS • WCS • NITF • JPEG 2000 • GML	Geospatial Data profile (u)	GML 3.1.1	OpenGIS Geography Markup Language Encoding Specification, 7 February 2004	M
			ISO/IEC 15444-1:2004 | ITU-T Rec. T.800	Information Technology -- JPEG 2000 image coding system: Core coding system	M
			ISO/IEC 15444-9:2005 w/Cor 1:2007, Cor 2:2008, Amd 1:2006	Information technology -- JPEG 2000 image coding system: Interactivity tools, APIs and protocols, November 17, 2005 with Cor 1:2007, Cor 2:2008, Amd 1:2006, Amd 2:2008, and Amd 3:2008	M
			MIL-STD-188-199(1)	Vector Quantization Decompression for the National Imagery Transmission Format Standard, 27 June 1994 with Notice 1, 27 June 1996	M
			MIL-STD-2500C	National Imagery Transmission Format (Version 2.1) for the National Imagery Transmission Format Standard, 01 May 2006	M
			NGA STDI-0001 v1.3/CN2	National Support Data Extensions (SDE) (Version 1.3/CN2) for the National Imagery Transmission Format (NITF), 10	M

Table 1 – Enterprise Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
				July 2007	
			OGC WCS 1.1.2	Web Coverage Service (WCS) Implementation Standard, Version 1.1.2 (v1.1 Corrigendum 2 release), 2008-03-19	M
			STDI-0002 v3	The Compendium of Controlled Extensio ns (CE) for the National Imagery Transmission Format (NITF), v3, 1 August 2007	M
			STDI-0006, 23 July 2008	National Imagery Transmission Format (NITF) Version 2.1 Commercial Dataset Requirements Document (NCDRD), 23 July 2008	M
			WFS 1.1	OpenGIS Web Feature Service (WFS) Implementation Specification	M
Runtime and App Library					
Frameworks	• Microsoft ASP .NET • Microsoft .NET Compact Framework • Common Language Runtime	Dot NET Framework			N
	• Apache Wicket • JavaServer Faces • J2EE	Java Framework			N
	• Apache Web Server • JBOSS Enterprise Middleware • J2EE - Java 2 Platform, Enterprise Edition	Open Source Framework			N
Image and Run-Time Environments	Army Golden Master	N/A		Army Standard Baseline Configurations for commonly used computing environment within the Army Enterprise Infrastructure	
Development Environments	• MS Visual Studio version X.X • Eclipse version X.X • Ozone	Development Environments			N
Ozone Widget Framework (OWF)	OWF/HTML, XML/WDSL/SOAP/UDDI, X.509/PKI, OWF widgets,	Ozone Widget Framework (OWF) Profile (u)	N/A	OWF-compliant web server functions (e.g. HTT server, HTTP client, javax.servlet container)	N
			N/A	OWF-compliant Synapse Common Data Model	N
			N/A	OWF-compliant Common Message Component	N
			N/A	OWF-compliant widget event model	N

			N/A	OWF-compliant Widgets Interconnection Interfaces (e.g. Battle Command [BC], 2D/3D Mapping, Symbology, Notepad Memo, SkiWeb, and airspace management)	N
			HTML 4.01	HTML 4.01 Specification, W3C Recommendation, revised, 24 Dec 1999	M
			XHTML 1.1: 31 May 2001	Extensible Hypertext Markup Language (XHTML) Version 1.1 - Module-based XHTML, W3C Recommendation, 31 May 2001	M
			IETF RFC 2616	Hypertext Transfer Protocol - HTTP 1.1, June 1999	M
			UDDI 3.0.2	OASIS Universal Description, Discovery, and Integration Version 3.0.2 UDDI Spec, Dated 2004-Oct-19	M
			W3C SOAP 1.2 Part 1	SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation 27 April 2007	M
			W3C SOAP 1.2 Part 2	SOAP 1.2 Part 2: Adjuncts (Second Edition), W3C Recommendation 27 April 2007	M
			WSDL 1.1	Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001	M
			XML 1.0 (Third Edition)	Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation, 04 February 2004	M
			OASIS CAP-V1.1	Common Alerting Protocol, v. 1.1, October 2005	E
			IETF RFC 2560	IETF Public Key Infrastructure X.509 (PKIX) Online Certificate Status Protocol (OCSP), RFC 2560, June 1999	M
			IETF RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999	M
			IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	M

			IETF RFC 2865	Remote Authentication Dial In User Services (RADIUS), June 2000	M
			IETF RFC 2589	Lightweight Directory Access Protocol (v3): Extensions for Dynamic Directory Services, June 2000	M
			IETF RFC 2849	The LDAP Data Exchange Format (LDIF), June 2000	M
			IETF RFC 3377	Lightweight Directory Access Protocol (v3): Technical Specification; September 2002	M
			IETF RFC 3673	Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes, December 2003	M
Reports, Interfaces, Conversions and Extensions (RICE) Framework	RICE Objects	Reports, Interfaces, Conversions and Extensions (RICE) Profile (p)	N/A	DoD RICE Repository Process, 8 July 2003	N
Widget Framework	Smart Google Web Toolkit (GWT). http://code.google.com/p/smartgwt/	N/A		Google Web Toolkit	
Operating System					
Operating Systems	• Windows 2003 Server (or newer) • Red Hat Enterprise Linux Server OS version 5 or higher	Operating Systems			N

Tactical Servers **–** characterized by server-class hardware paired with powerful client workstations connected by a generally reliable network with moderate to high bandwidth in tactical tent or improved building environments. This allows command post mission environment users and systems to leverage capabilities offered by the enterprise, as well as to operate robust capabilities locally. The services and standards for tactical servers are detailed below in Tables 2 and 3.

Table 2 – Tactically Hosted Enterprise Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Standard Applications					
User Support	This is a NEC service (e.g. Army Golden Master: Remote Access, SW updates/patches/hotfixes, Anti-Virus/Spyware)	N/A		Army Standard Baseline Configurations for commonly used computing environment within the Army Enterprise Infrastructure.	
Training	Learning Technology Systems Architecture (LTSA)	Learning Management Services	IEEE 1484.11.1-2004	Standard for Learning Technology - Data Model for Content Learning Management System Communication, January 1, 2005	M
			IEEE 1484.1-2003	Standard for Learning Technology-Learning Technology Systems Architecture (LTSA), February 1, 2003	M
	Modeling and Simulation (M&S) High Level Architecture (HLA)	Modeling & Simulation Services	IEEE 1320.1	IEEE Standard for Functional Modeling Language-Syntax and Semantics for IDEF0. March 24, 2004 (reaffirmed)	M
			IEEE 1320.2	Conceptual Modeling Language - Syntax and Semantics for IDEF1X97 (IDEF object), 1998	M
			IEEE 1516	IEEE 1516-2000 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Framework and Rules	M
			IEEE 1516.1	IEEE 1516.1-2000 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Federate Interface Specification	M
			IEEE 1516.2	IEEE 1516.2-2000 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Object Model Template (OMT) Specification	M
	• Data Model for Content Learning Management System Communication • Modeling and Simulation (M&S) High Level Architecture (HLA)	Virtual Environment Training profile (p)	IEEE 1484.11.1-2004	Standard for Learning Technology - Data Model for Content Learning Management System Communication, January 1, 2005	M
			IEEE 1516	IEEE 1516-2000 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Framework and Rules	M
Workflow Engine	• jBPM • Apache ODE • Red Hat	Workflow Engine			N
Redirection	HTTP	Hyper Text Transfer Protocol (HTTP)	IETF RFC 2616	Hypertext Transfer Protocol - HTTP 1.1, June 1999	M
Metadata Registry	DDMS	Content Discovery profile (p)	DDMS 2.0	Department of Defense Discovery Metadata Specification (DDMS), Version 2.0, 17 July 2008	M
M2M Messaging	Variable Message Format (VMF)	Military C2 Messages profile (u)	MIL-STD-6017B	Variable Message Format (VMF), June 2009	M
Service	This is part of DISA	N/A		PM leverages DISA services.	

Table 2 – Tactically Hosted Enterprise Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Discovery	Standards-Based Enterprise Services http://www.disa.mil/nces/ (see NCES 101 Briefing Slides for details)				
Content Discovery Enterprise Search	This is part of DISA Standards-Based Enterprise Services http://www.disa.mil/nces/ (see NCES 101 Briefing Slides for details)	N/A		PM leverages DISA services.	
SkiWeb	• OASIS WS-Base Notification 1.3 • OASIS WS-Brokered Notification 1.3	Web Eventing / Notification Services	OASIS WS-Base Notification 1.3	Web Services Base Notification 1.3 (WS-Base Notification), OASIS Standard, 1 October 2006	M
			OASIS WS-Brokered Notification 1.3	Web Services Business Activity (WS-Business Activity), Version 1.1, OASIS Standard incorporating Approved Errata, 12 July 2007	M
	WS-Eventing	Web Services Eventing	WS-Eventing	Web Services Eventing (WS-Eventing), August 2004	E
Collaboration	DCO https://www.dco.dod.mil/	N/A		Army standardized collaboration service	
Enterprise Service Management	This is part of DISA Standards-Based Enterprise Services http://www.disa.mil/nces/ (see NCES 101 Briefing Slides for details)	N/A		PM leverages DISA services.	
GCDS	This is a DISA GIG Content Delivery Service http://www.disa.mil/gcds/index.html	N/A		PM leverages DISA services.	
Social Networking	Web 2.0 (e.g. Facebook)	Social Networking			N
Mediation	This is part of DISA Standards-Based Enterprise Services http://www.disa.mil/nces/ (see NCES 101 Briefing Slides for details)	N/A		PM leverages DISA services.	
GVS	Geospatial Intelligence Visualization Services Suite (e.g. GoogleGlobe, GoogleMaps) http(s)://gvshome.nga.smil.mil http(s)://gvsgooglemaps.nga.smil.mil http(s)://gvsgoogleglobe.nga.smil.mil	N/A		PM leverages NGA services.	
Security Configuration					
Security Services	ITU-T X.509	Implement NSA or NIST Public Key Cryptography	FIPS Pub 197	Advanced Encryption Standard (AES), 26 November 2001	M
			IETF RFC 2560	IETF Public Key Infrastructure X.509	M

Table 2 – Tactically Hosted Enterprise Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
		profile (u)		(PKIX) Online Certificate Status Protocol (OCSP), RFC 2560, June 1999	
			IETF RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999	M
			IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	M
			ITU-T X.509:2005	Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, August 2005	M
			PKIKMITKNPP	Public Key Infrastructure and Key Management Infrastructure Token (Medium Robustness) PP	M
	TLS	Web Services Security (WS Security) profile (p)	IETF RFC 4346	The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006	M
			IETF RFC 4347	Datagram Transport Layer Security, April 2006	M
			SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	M
			WS-Security 1.1	Web Services Security v1.1, February 2006	M
Runtime and App Library					
Widget Framework	Smart Google Web Toolkit (GWT). http://code.google.com/p/smartgwt/ Ozone widgets (see Ozone Widget Framework – TAB 1 Table 1 - Enterprise Server Standards)	N/A		Google Web Toolkit	
Image and Runtime Environments	Army Golden Master	N/A		Army Standard Baseline Configurations for commonly used computing environment within the Army Enterprise Infrastructure.	
Development Environments	• MS Visual Studio version X.X • Eclipse version X.X • Ozone	Development Environments			N
Orchestration Engine	• Apache ODE • NetBeans Enterprise Pack	Orchestration Engine			N
Operating Systems					
Operating Systems	• Windows 2003 Server (or newer) • Red Hat Enterprise Linux Server OS version 5 or higher	Operating Systems			N

Table 3 – Tactical (BCCS) Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Standard Applications					
Workflow Engine	• BPM • Apache ODE • Red Hat	Workflow Engine			N
Redirection	HTTP	Hypertext Transfer	IETF RFC 2616	Hypertext Transfer	M
M2M Messaging	Variable Message Format (VMF)	Military C2 Messages profile (u)	MIL-STD-6017B	Variable Message Format (VMF), June 2009	M
Content Discovery Enterprise Search	This is part of DISA Standards-Based Enterprise Services http://www.disa.mil/nces/ (see NCES 101 Briefing Slides for details)	N/A		PM leverages DISA services.	
Collaboration	DCO https://www.dco.dod.mil/	N/A		Army standardized collaboration service	
Geospatial Maps and Products	Commercial Joint Mapping Toolkit (CJMTK) http://www.cjmtk.com	Commercial Joint Mapping Tool Kit (CJTMK) Profile (u)	BML	Battle Management Language (BML)	N
			WFS 1.1	Geospatial Battle Management Language (GeoBML)	N
			GML 3.1.1	OpenGIS Geography Markup Language Encoding Specification, 7 February 2004	M
			ISO 19136:2007	Geographic information -- Geography Markup Language, 2007-08-23	M
			MIL-STD-2407(1)	Interface Standard for Vector Product Format (VPF), 28 June 1996, with Notice of Change, Notice 1, 26 October 1999	M
			MIL-STD-2411(2)	Raster Product Format, 6 October 1994; with Notice of Change, Notice 1, 17 January 1995, and Notice of Change, Notice 2, 16 August 2001	M
			MIL-STD-2411-1 w/Chg 3	Registered Data Values For Raster Product Format, 30 August 1994; with Change 3, 1 December 2009	M
			MIL-STD-2525C	Common Warfighting Symbology, 17 November 2008	M
			WFS 1.1	OpenGIS Web Feature Service (WFS) Implementation Specification	M
			WMS 1.3	OpenGIS Web Map Service (WMS) Implementation Specification, Version 1.3, 15 March 2006	M
	• Google Earth	N/A		Google Earth	
	•				
Security Configuration					
Security Services	ITU-T X.509	Implement NSA or NIST Public Key Cryptography profile (u)	FIPS Pub 197	Advanced Encryption Standard (AES), 26 November 2001	M
			IETF RFC 2560	IETF Public Key Infrastructure X.509 (PKIX) Online Certificate Status Protocol (OCSP), RFC 2560, June 1999	M
			IETF RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999	M

Table 3 – Tactical (BCCS) Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
			IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	M
			ITU-T X.509:2005	Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, August 2005	M
			PKIKMITKNPP	Public Key Infrastructure and Key Management Infrastructure Token (Medium Robustness) PP	M
	WS-Security	Web Services Security (WS Security) profile (p)	IETF RFC 4346	The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006	M
			IETF RFC 4347	Datagram Transport Layer Security, April 2006	M
			SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	M
					M
			WS-Security 1.1	Web Services Security v1.1, February 2006	M
	Java Authentication and Authorization Service (JAAS) http://java.sun.com/javase/technologies/security/	N/A		Java Security Services	
Geospatial Visualization	• WMS • WFS • WCS • WMC • KML • GML • NITF • JPEG 2000 • RPF	Geospatial Visualization Services profile (u)	GML 3.1.1	OpenGIS Geography Markup Language Encoding Specification, 7 February 2004	M
			ISO/IEC 15444-1:2004 | ITU-T Rec. T.800	Information Technology -- JPEG 2000 image coding system: Core coding system	M
			ISO/IEC 15444-9:2005 w/Cor 1:2007, Cor 2:2008, Amd 1:2006	Information technology -- JPEG 2000 image coding system: Interactivity tools, APIs and protocols, November 17, 2005 with Cor 1:2007, Cor 2:2008, Amd 1:2006, Amd 2:2008, and Amd 3:2008	M
			NGA STDI-0001 v1.3/CN2	National Support Data Extensions (SDE) (Version 1.3/CN2) for the National Imagery Transmission Format (NITF), 10 July 2007	M
			OGC WCS 1.1.2	Web Coverage Service (WCS) Implementation Standard, Version 1.1.2 (v1.1 Corrigendum 2 release), 2008-03-19	M
			STDI-0002 v3	The Compendium of Controlled Extensio ns (CE) for the National Imagery Transmission Format (NITF), v3, 1	M

Table 3 – Tactical (BCCS) Server Standards					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
				August 2007	
			STDI-0006, 23 July 2008	National Imagery Transmission Format (NITF) Version 2.1 Commercial Dataset Requirements Document (NCDRD), 23 July 2008	M
			WFS 1.1	OpenGIS Web Feature Service (WFS) Implementation Specification	M
			WMC 1.1	OpenGIS Web Map Context (WMC) Documents Implementation Specification, Version 1.1.0, 19 January 2005	M
			WMS 1.3	OpenGIS Web Map Service (WMS) Implementation Specification, 2 August 2004	M
				KML (Keyhole Markup Language) 2.2 – An OGC Best Practice	N
				RPF/CADRG (Raster Product Format/Compressed ADRG) MILPRF-89038	N
Runtime and App Library					
Image and Run-Time Environments	Army Golden Master	N/A		Army Standard Baseline Configurations for commonly used computing environment within the Army Enterprise Infrastructure.	
Development Environments	• MS Visual Studio version X.X • Eclipse version X.X • Ozone	Development Environments			N
Frameworks	Microsoft ASP .NET	Dot NET Framework			N
	Ozone (see Ozone Widget Framework – TAB 1 Table 1 - Enterprise Server Standards)	Ozone Widget Framework			
	• Apache Wicket • JavaServer Faces • J2EE	Java Framework			N
	• Apache Web Server • JBOSS Enterprise Middleware • J2EE - Java 2 Platform, Enterprise Edition	Open Source Framework			N
Orchestration Engine	• Apache ODE • NetBeans Enterprise Pack	Orchestration Engine			N
Operating Systems					
Operating Systems	• Windows 2003 Server (or newer) • Red Hat Enterprise Linux Server OS version 5 or higher	Operating Systems			N

TAB 2: Client (Tactical) Standards

Client **–** an end-user system typically running on a laptop in a tactical environment (Battle Command Workstation). The services and standards for clients are detailed in Table 1, below.

Table 1 – Client Standards for BC Workstation					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Standard Application					
Banner	Army Golden Master (e.g. Lengths/Sizes of Text & Image)	N/A		Army Standard Baseline Configurations for commonly used computing environment within the Army Enterprise Infrastructure.	
M2M Messaging	VMF	Military C2 Messages profile (u)	MIL-STD-6017B	Variable Message Format (VMF), June 2009	M
Chat	XMPP	Instant Messaging (IM) profile (p)	IETF XMPP	Extensible Messaging and Presence Protocol, December 2004	M
Office Products	Office Open XML	Office Products	ISO/IEC 29500-1:2008	Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference, First edition, 2008-11-15	E
			ISO/IEC 29500-2:2008	Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 2: Open Packaging Conventions, First edition, 2008-11-15	E
			ISO/IEC 29500-3:2008	Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 3: Markup Compatibility and Extensibility, First edition, 2008-11-15	E
			ISO/IEC 29500-4:2008	Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 4: Transitional Migration Features, First edition, 2008-11-15	E
Frameworks	Microsoft ASP.NET	Dot NET Framework			N
	Ozone (see Ozone Widget Framework – TAB 1 Table 1 - Enterprise Server Standards)	Ozone Widget Framework			N

Table 1 – Client Standards for BC Workstation					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
	•				
Geospatial Maps and Products	• Commercial Joint Mapping Toolkit (CJMTK) Profile (u) http://www.cjmtk.com	Commercial Joint Mapping Tool Kit (CJTMK) profile (u)	BML	Battle Management Language (BML)	N
			GeoBML	Geospatial Battle Management Language (GeoBML)	N
			GML 3.1.1	OpenGIS Geography Markup Language Encoding Specification, 7 February 2004	M
			ISO 19136:2007	Geographic information -- Geography Markup Language, 2007-08-23	M
			MIL-STD-2407(1)	Interface Standard for Vector Product Format (VPF), 28 June 1996, with Notice of Change, Notice 1, 26 October 1999	M
			MIL-STD-2411(2)	Raster Product Format, 6 October 1994; with Notice of Change, Notice 1, 17 January 1995, and Notice of Change, Notice 2, 16 August 2001	M
			MIL-STD-2411-1 w/Chg 3	Registered Data Values For Raster Product Format, 30 August 1994; with Change 3, 1 December 2009	M
			MIL-STD-2525C	Common Warfighting Symbology, 17 November 2008	M
			WFS 1.1	OpenGIS Web Feature Service (WFS) Implementation Specification	M
			WMS 1.3	OpenGIS Web Map Service (WMS) Implementation Specification, Version 1.3, 15 March 2006	M
	• Google Earth	N/A		Google Earth	N
Security Configuration					
Security Services	ITU-T X.509	Implement NSA or NIST Public Key Cryptography profile (u)	FIPS Pub 197	Advanced Encryption Standard (AES), 26 November 2001	M
			IETF RFC 2560	IETF Public Key Infrastructure X.509 (PKIX) Online Certificate Status Protocol (OCSP), RFC 2560, June 1999	M
			IETF RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999	M
			IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	M
			ITU-T X.509:2005	Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, August 2005	M
			PKIKMITKNPP	Public Key Infrastructure and Key Management Infrastructure Token (Medium Robustness) PP	M
	WS-Security	Web Services Security (WS Security) profile (p)	IETF RFC 4346	The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006	M
			IETF RFC 4347	Datagram Transport Layer Security, April 2006	M
			SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	M

Table 1 – Client Standards for BC Workstation					
Services	**Standards**	**TRM Std Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
			WS-Security 1.1	Web Services Security v1.1, February 2006	M
Runtime & APP Library					
Runtime	JAVA Runtime Environment version X	Runtime			N
Image and Runtime Environments	Army Golden Master	N/A		Army Standard Baseline Configurations for commonly used computing environment within the Army Enterprise Infrastructure.	
Operating System					
Operating System	Windows Vista or higher* (*Army/NETCOM must approve any OS higher than Vista)	Operating System			N

TAB 3: Platform Standards

Platform **–** a reduced network, computing, environmental and form-factor context, to include size, weight, power and cost (SWAP-C) considerations. For platforms, the path forward in the long term must provide the tailoring and flexibility demanded by smaller form factors and limited bandwidth.

Table 1 – Platform Computing Environment Standards					
Services	**Standards**	**TRM Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Standard Application					
Geospatial maps and products - CJMTK or compatible	Visualization	Commercial Joint Mapping Toolkit (CJMTK) Profile (u)	BML	Battle Management Language (BML)	N
			GeoBML	Geospatial Battle Management Language (GeoBML)	N
			GML 3.1.1	OpenGIS Geography Markup Language Encoding Specification, 7 February 2004	M
			ISO 19136:2007	Geographic information -- Geography Markup Language, 2007-08-23	M
			MIL-STD-2407(1)	Interface Standard for Vector Product Format (VPF), 28 June 1996, with Notice of Change, Notice 1, 26 October 1999	M
			MIL-STD-2411(2)	Raster Product Format, 6 October 1994; with Notice of Change, Notice 1, 17 January 1995, and Notice of Change, Notice 2, 16 August 2001	M
			MIL-STD-2411-1 w/Chg 3	Registered Data Values For Raster Product Format, 30 August 1994; with Change 3, 1 December 2009	M
			MIL-STD-2525C	Common Warfighting Symbology, 17 November 2008	M
			WFS 1.1	OpenGIS Web Feature Service (WFS) Implementation Specification	M
			WMS 1.3	OpenGIS Web Map Service (WMS) Implementation Specification, Version 1.3, 15 March 2006	M
Chat interface - protocol suitable for network conditions		Instant Messaging (IM) profile (p)	IETF XMPP	Extensible Messaging and Presence Protocol, December 2004	M
Browser – products compliant with open standards	• MS Internet Explorer • Mozilla Firefox	Web Browser			N
Adobe Acrobat document viewer – product	Adobe Acrobat Documents Viewer	Document Viewer			N
Office Products	Office Open XML	Office Products	ISO/IEC 29500-1:2008	Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference, First edition, 2008-11-15	E
			ISO/IEC 29500-2:2008	Information technology -- Document description and processing languages --	E

Table 1 – Platform Computing Environment Standards					
Services	**Standards**	**TRM Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
				Office Open XML File Formats -- Part 2: Open Packaging Conventions, First edition, 2008-11-15	
			ISO/IEC 29500-3:2008	Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 3: Markup Compatibility and Extensibility, First edition, 2008-11-15	E
			ISO/IEC 29500-4:2008	Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 4: Transitional Migration Features, First edition, 2008-11-15	E
Security Configuration					
Encryption of data at rest		Encryption	FIPS Pub 197	Advanced Encryption Standard (AES), 26 November 2001	M
			FIPS Pub 198	Federal Information Processing Standard Publication 198, Keyed-Hash Message Authentication Code, March 6, 2002	M
		Implement NSA or NIST Public Key Cryptography	IETF RFC 2560	IETF Public Key Infrastructure X.509 (PKIX) Online Certificate Status Protocol (OCSP), RFC 2560, June 1999	M
Multiple independent levels of security	Army Golden Master	N/A		Army Standard Baseline Configurations for commonly used computing environment within the Army Enterprise Infrastructure	
Anti-virus	• • Symantec	N/A		Army Standard Baseline Configurations for commonly used computing environment within the Army Enterprise Infrastructure	
Standard Security Policy		IP Security Policy Management	IETF RFC 3585	IPsec Configuration Policy Information Model, Aug 2003	M
Identity Management (IdM)		Biometric	ISO/IEC 7816-11:2004	ISO/IEC 7816-11:2004 - Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods	M
			NIST Special Publication 800-76-1	Biometric Data Specification for Personal Identity Verification, January 2007	M
			DoD EBTS v2.0	Department of Defense (DoD) Electronic Biometric Transmission Specification, Version 2.0, 27 March 2009	M
			ISO/IEC 19794-6:2005	Information technology - Biometric data interchange formats - Part 6: Iris image data, 10 June 2005	M
Runtime & App Library					
Development Environments by Third Parties			JSR-168	Java Specification Request (JSR) JSR-168, Portlet Specification API, Final Release ballot, Version 1.0, 06 October 2003	M
			JSR-914	Java Specification Request (JSR) JSR-914 Java Message Service (JMS) API, Final Release, Version 1.1, April 12, 2002	M

Table 1 – Platform Computing Environment Standards					
Services	**Standards**	**TRM Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
	Java APIs JAIN, http://java.sun.com/products/jain/index.html	Open APIs			N
	Parlay APIs The Parlay Group, "Parlay specifications 3.0", http://www.parlay.org/specs/	Parlay APIs			N
		Biometrics APIs	ISO/IEC 24709-1:2007	Conformance testing for the biometric application programming interface (BioAPI) - Part 2: Test assertions for biometric service providers, 2007-02-02	M
			ISO/IEC 24709-1:2007	Conformance testing for the biometric application programming interface (BioAPI) - Part 1: Methods and Procedures, 2007-01-29	M
Software Development Kit (SDK)	• Microsoft ASP .NET • Microsoft .NET Compact Framework	Dot NET Framework			N
Platform-specific libraries and components	• JAVA Library • Versatile Information Systems Integrated On-Line (VISION) Library	N/A		Library Services	
Standard Install/Image and Runtime Environments	• Over-the-Air Patch • JAVA Runtime Environment	N/A		Install/Image and Runtime Environments.	
Operating System					
Standard Operating Systems	• Windows 2003 Server (or newer) • Red Hat Enterprise Linux Server OS version 5.0 or higher	Operating System			N

The platform computing environment shall use unmodified COTS software to the maximum extent possible in order to adapt as technology evolves and quickly respond to user needs.

The platform computing environment shall be developed, licensed and procured in a manner that enables use by our Joint and multinational mission partners.

The platform computing environment shall separate the transport layer from applications and automatically configure/initialize to the available transport. The platform OE must support existing and emerging transport.

All platform applications shall use common components (e.g., common displays, time, network access, location services) in order to improve SWAP-C. Standard interfaces and open standards shall be used to enable continuous modernization and to reduce system re-set and upgrade/life-cycle costs.

- Security:
    - Encryption of data at rest
    - Multiple independent levels of security to support users with and without Secret clearances
    - Anti-virus (this requirement does not apply to weapons systems using a Real-Time Operating System)
    - Standard Security Policy
    - Identity Management (IdM)
- Standard Operating Systems:
    - Red Hat Enterprise Linux Server OS version 5.0 or higher
    - Windows 2003 Server (or newer)
    - Real-Time OS (RTOS) for embedded weapons platforms
- Development Environments:
    - Support development by third parties so that features can be added and platform variants can be developed.
    - Commercial SDK
    - Geospatial maps and products – CJMTK or compatible
    - Platform-specific libraries/components provide a common, managed set of features that can be reused by third parties.
- Standard Install/Image and Runtime Environments:
    - Over-the-air patch
    - JAVA Runtime Environment

- Standard Applications (subject to operational requirements)
    - Chat interface – protocol suitable for network conditions
    - Browser – product
    - Adobe Acrobat document viewer – product
    - Microsoft Office-compatible document editor – product
    - Microsoft Office-compatible presentation editor – product

TAB 4: Mobile Standards

Mobile **–** characterized by small handheld devices. The technologies for this environment are based on lightweight hand-held computing and communications devices (e.g., an "industry leader" COTS Smartphone platform).

Table 1 – Mobile Computing Environment Standards					
Services	**Standards/ Technologies**	**TRM Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Security Configuration					
Security	Army, DISA and NSA Security Technical Implementation Guide (STIG) http://iase.disa.mil/stigs/checklist/index.html	N/A		PM leverages DISA services. .	
Runtime & App Library					
Mobile Software Development Kits (SDK)	• iPhone • RIM • Android	Mobile Software Development Kits			N
Operating System					
Mobile Operating Systems (OS)	• iOS (previously iPhone OS) • Research in Motion (RIM) OS • Android OS	Mobile Operating Systems			N

Smartphone products are rapidly evolving. To keep pace, development life cycles should be short (6-12 months) and use development kits provided for the Smartphone.

Army-specific hardware, operating systems and development toolkits being developed in this space shall be reconsidered to determine whether emerging Smartphone and slate technologies can more efficiently and effectively support the requirements.

Though more than 90 percent of Army-issued handheld devices are Blackberry devices (Research in Motion), the Smartphone market is rapidly evolving. A single vendor cannot be determined at this time. Gartner predicts[5] that the Smartphone OS market will remain fragmented for the next three years. RIM and Apple continue to dominate the market, but increased competition, particularly from Android-based devices, will cause changes to market share over time. For applications that require multitasking, the Android OS is the top performer. For applications that require rich graphical images and a multi-touch user interface, the iPhone OS offers the best option. If security is a driving factor, the leader is Blackberry.

---

[5] Competitive Landscape: Smartphone Operating Systems, Gartner, 8 December 2009.

- Standard Operating Systems:
    - iPhone OS
    - Android OS
    - Research in Motion (RIM) OS
- Development Environments:
    - iPhone SDK
    - Android SDK
    - RIM SDK

Security:

- Security configuration shall comply with appropriate STIGs.

TAB 5: Sensor Standards

Sensors **–** specialized, human-controlled or unattended computing environments. Sensors are organized by family (e.g., material detection, video surveillance, task robot), with different characteristics and capabilities based on mission requirements.

Table 1 – Sensor Computing Environment Standards					
Services	**Standards/ Technologies**	**TRM Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Standard Application					
Sensor Device / Transducer Interfaces		Sensor Device / Transducer Interfaces	IEEE 1451.0	Smart Transducer Interface for Sensors and Actuators — Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats	N
			IEEE 1451.2	Smart Transducer Interface for Sensors and Actuators–Transducer to Microprocessor Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats	N
			IEEE 1451.4	Smart Transducer Interface for Sensors and Actuators—Mixed-Mode Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats	N
			IEEE 1451.5	Smart Transducer Interface for Sensors and Actuators– Wireless Communication and Transducer Electronic Data Sheet (TEDS) Formats	N
			IEEE 1451.7	Smart Transducer Interface for Sensors and Actuators - Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats	N
Sensor Network Interface (Smart Web Services)		Sensor Network Interface	IEEE P1451.1 HTTP Services	HTTP Services	N
			IEEE P1451.1 Web Services	Web Services (Smart Transducer Web Services)	N
			IEEE P1451.1 IP Services	IP Services	N
Sensor Application Data Format		Sensor Application Data Format	ANSI N42.42	ANSI N42.42	N
			CBRNE Data Model	CBRNE Data Model (in collaboration with JPEO Data Model Working Group)	N
			OASIS CAP-V1.1	Common Alerting Protocol, v. 1.1, October 2005	E
			OASIS EDXL-DE	OASIS EDXL-DE	N
			OGC OMXML	OGC's Observations & Measurements (O&M- OMXML)	N
			OGC SensorML v1.0.0	OpenGIS Sensor Model Language (SensorML) Implementation Specification, Version 1.0.0 [OGC 07-000], 17 July 2007	M

Table 1 – Sensor Computing Environment Standards					
Services	**Standards/ Technologies**	**TRM Profiles**	**Standard ID**	**Standard Title**	**DISR Status**
Sensor Application Services		Sensor Application Services	OpenGIS SOS 1.0	OpenGIS Sensor Observation Service Implementation Specification, Version 1.0, 26 October 2007	M
			SAS	Sensor Alert Service (SAS)	N
			SPS 1.0	OpenGIS Sensor Planning Service Implementation Specification, 2007-08-02	M
			CAT 2.0.2	OpenGIS Catalogue Service (CAT) Implementation Specification (2.0.2), 23 February 2007	M
			WPS 1.0	OpenGIS Web Processing Service, 2007-06-08	M
Operating System					
Sensor Operating Systems (OSs)		N/A		Sensor Operating Systems (OSs)	

While the development of sensors and wireless sensor networks was originally motivated by military applications, such as battlefield surveillance, they are now used in many industrial and civilian areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation and traffic control. The sensor industry ecosystem is vibrant. iRobot products run a robot intelligence system based on Linux and have open Application Programming Interfaces (APIs) so that third parties can develop for their robots. Approximately 80 companies and organizations attended the 2009 developer conference to learn how to develop capabilities for iRobot robots[6]. In one example of commercial collaboration, iRobot integrated a third-party TNT-sniffing function into one of its robots to meet the requirements of a military contract.

The diversity of commercial industry sensor work indicates that the Army can and should leverage commercial technology for its sensor computing environments, and should look to commercial technology before developing unique/custom technology.

Operating systems (OSs) for sensors are less complex than general-purpose Oss, both because of the special requirements of sensor applications and the resource constraints in sensor hardware platforms. Sensor applications are usually not interactive in the same way as applications for PCs. The OS therefore does not need to include support for user

[6] Insights on a Future Growth Industry: An Interview with Colin Angle, CEO, iRobot. Gartner, 8 January 2010.

interfaces. Furthermore, resource constraints, in terms of memory and memory mapping hardware support, make mechanisms such as virtual memory either unnecessary or impossible to implement.

Sensor hardware is not different from traditional embedded systems and, therefore, it is possible to use embedded OSs. Unlike traditional embedded OSs, however, OSs specifically targeting sensor networks often do not have real-time support.

TinyOS (a free and open source component-based OS) is specifically designed for wireless sensor networks. Unlike most other operating systems, TinyOS is based on an event-driven programming model instead of multi-threading. TinyOS programs are built out of software components, some of which present hardware abstractions. Components are connected to each other using interfaces. TinyOS provides interfaces and components for common abstractions, such as packet communication, routing, sensing, actuation and storage.

There are other sensor-appropriate OSs that allow programming in C. Examples of such OSs include Contiki, MANTIS, BTnut, SOS and Nano-RK. LiteOS is a newly developed OS for wireless sensor networks that provides UNIX-like abstraction and support for the C programming language.

The overall conclusion is that commercial technology exists for the sensor computing environment and the Army will leverage COTS technology to the maximum extent possible when developing and fielding in the sensor computing environment.

TAB 6: Program Maturity Model Criteria

Development Attributes

Table 1 - Architecture Standardization Measures a technology's conformity to a defined set of architectural standards.	
Level 1	Technology is selected to support the local needs of the user/customer. Use of existing technology is encouraged but not a driving factor.
Level 2	Technology that is compatible with the current computing configuration is given top priority. Applications that require unique technology are developed as needed.
Level 3	The Army's technology architecture has been standardized; therefore, exceptions require approval. Technology conforms to the Army's technology architecture standards.
Level 4	Technology conforms to Joint/Coalition technology architecture standards that stress component re-use, interoperability and agility. All functionality is delivered from a standardized development environment.

Table 2 - Development Process Measures the relative maturity of software development processes and how well development teams conform to standards.	
Level 1	Development teams adhere to the set of processes and standards defined by the development organization.
Level 2	Development teams adhere to local standards and procedures. Development teams produce the same artifacts as dictated by the local policy.
Level 3	Development teams use Army standardized tools, methods and procedures for the technology. The technology is available within the DISA Rapid Access Computing Environment (RACE) for developers to stage new software.
Level 4	Development teams use Joint/Coalition standardized tools, methods and procedures for the technology. The technology is available within the DISA Rapid Access Computing Environment (RACE) for developers to develop, test and stage new software.

Table 3 - Software Development Toolkit (SDK)/Integrated Development Environment (IDE) Scope of Use Assesses the degree to which standardized software development environments are used for building new software.	
Level 1	IDEs/SDKs are many and are left to the discretion of the developer. Each technology has a unique set of development tools. Some SDKs are coupled with the applications. Applications created by the various IDEs/SDKs are designed to run locally and are not intuitively compatible with other environments.
Level 2	A standard set of Army-approved IDEs/SDKs exists for each technology within a specific computing environment. The number of unique programming languages supported by each platform is limited to a defined few. All software developed in the technology adheres to a strict set of standards designed specifically for developing within a standard configuration.
Level 3	A standard set of DoD-approved IDEs/SDKs exists for each technology spanning multiple computing environments. All systems are developed using the same tools and standards.
Level 4	A standard set of commercially available IDEs/SDKs exists for each technology inside and outside the DoD network. All software is developed using the same industry best-practices tools and standards.

Table 4 - Component Reuse Assesses the maturity of the software development process to proactively design, build and utilize reusable code and components in all development initiatives.	
Level 1	Software code and components are developed to satisfy a specific function and are bound to the technology in which they are developed. There are no reusable Army software components and no method in place to reuse them.
Level 2	Software code and components are developed using a common IDE/SDK and can be shared among applications that were developed using the same IDE/SDK or that use compatible technology. There is a library where reusable code and software components are stored, but new functionality is not routinely packaged into reusable components.
Level 3	Software is designed to be reusable. Libraries containing reusable components exist for each development technology. New development combines existing software components and new components to create applications.
Level 4	Enterprise-wide component libraries exist. Components and services have been cataloged, validated and certified. All new development includes existing software components whenever possible. Development of duplicate functionality is not permitted.

Table 5 - Information Assurance (IA) Assesses how IA/security is designed and built into all new technology decisions and deployments.	
Level 1	Security considerations are not part of software design. Certification and Accreditation (C&A) requires examination of all components of the development environment and all components of any applications developed within the development environment. Software does not integrate any user login or account privileges.
Level 2	Security is considered but built in after software has been developed. C&A requires examination of some components of the development environment and all components of any applications developed within the development environment. Software requires a separate user login with extensive account/service privileges.
Level 3	Security assessment and design are performed as part of routine software design reviews. The development environment has been certified and as such does not require examination for C&A. A limited number of reusable application components has been certified and any other application components require examination for C&A. Software uses local OS identity model.
Level 4	All new development adheres to a well-defined set of security guidelines throughout the design and development process. Both the development environment and a large number of reusable application components have been certified to enable rapid development using the technology. Software integrates with DoD identity model.

Deployment Attributes

Table 6 - System Coupling Assesses the dependence of one technology on another, with increased operability and compatibility being the ultimate goal.	
Level 1	Applications are tightly bound to the technology in which they are developed and cannot be shared with other technologies. Hardware and software are fully integrated.
Level 2	Applications are bound to the technology in which they are developed as part of a standard image (Army Golden Master).
Level 3	Applications are compatible with various hardware configurations. Moving applications and information between configurations is possible. Applications built in one technology can be run on another technology.
Level 4	Enterprise applications are managed centrally. An Applications Marketplace of approved applications exists for the identified computing environments.

Table 7 - Organizational Reach Determines how and where key technology decisions are made and who has access to the technology.	
Level 1	Technology is deployed specific to the needs of a functional community.
Level 2	Technology priorities are determined at the Army enterprise level.
Level 3	Technology priorities are determined at the DoD level. Functionality is developed on a standard configuration allowing cross-service access.
Level 4	Technology is deployed to interact with existing Coalition technology. Interfaces are designed to allow the flow of information through the entire coalition network. U.S.-releasable code/components are separable so that a mission partner's capability can be maintained.

Table 8 - Availability of Capability and Data Assesses the reach across the enterprise of user capability/functionality and of production data.	
Level 1	Information is stored via direct attached devices. Data is exchanged via "point to point" solutions. Only systems that have physical access to the device can access the data directly and registration is limited within appropriate registries (Authoritative Data Sources, Metadata Registry, etc.). Standards are informal and loosely enforced. Data must be packaged and physically transferred to be shared.
Level 2	Data and functionality are locally available via the LAN. Little or no capability exists to access data from remote locations. Development is performed by groups linked by the LAN. Standards and processes are in place for cross-LAN development. Programs of Record/Systems of Record have transition plans to expose data as a web service.
Level 3	Data are made available via services or databases that are registered in accordance with DoD guidance, trusted and accessible within the Army LandWarNet.
Level 4	Data are made available via services or databases that are registered in accordance with DoD guidance, trusted and ubiquitous (accessible across the DoD Global Information Grid).

Table 9 - Information Sharing Coupling Assesses the availability of reliable enterprise production data to a system user. Determines the extent to which data are duplicated and/or isolated.	
Level 1	Most data are local. Data from outside the local environment must be selected and extracted from remote locations and inserted into the local environment to be processed. Only local data are considered "real time." Time lag can be significant and irregular.
Level 2	Data from remote locations are extracted and loaded locally on a regular basis. Though time lag can be significant, data are loaded on a regular schedule. Most data are maintained locally.
Level 3	Authoritative data sources are available and used. Data exist in numerous instances across the network. Synchronization of data sources is performed regularly. Some data are still maintained locally.
Level 4	A single instance of production data is maintained. Remote locations can access critical data at network speeds. The single instance is updated in "real time." The enterprise is moving towards data warehouses with connectivity to everyone on the network.

Table 10 - Presence and Sustainment Measures the maturity of on-going funding and maintenance. Considers market share and continued viability.	
Level 1	Technology does not have defined sustainment (support and funding) models in place. Support is ad hoc and reactive. Technology market presence and ecosystem are embryonic.
Level 2	Support estimates are defined in the initial requirements. Support sourcing and funding receive an annual review. Training is informal and supplied as needed. Technology undergoes periodic review to ensure that the capability still supports the mission and is being used in the field. Technology market presence and ecosystem are developing.
Level 3	Support and funding have been defined. Regular system upkeep is performed to keep systems viable and relevant. Attention is given to monitoring use in the field. Specific training is provided by the developer and included pre-deployment. Technology market presence and ecosystem are stable.
Level 4	Support funding is in place. Application viability is reviewed annually, with adjustments made to support needs and on-going funding. Use in the field is measured and evaluated. Training has been institutionalized using current Army training standards and techniques. Technology market presence and ecosystem are robust.

TAB 7: Acronyms

The acronyms used in this appendix are listed in the Table below.

Acronyms	
Acronym	**Description**
AGM	Army Golden Master
APC	Area Processing Centers
APIs	Application Programming Interfaces
BC	Battle Command
BCCS	Battle Command Common Services
C&A	Certification and Accreditation
C2	Command and Control
CDS	Cross-Domain Solutions
CE	Computing Environment
CMM	Capability Maturity Model
COCOM	Combat Commander
COE	Common Operating Environment
COP	Common Operating Picture
COTS	Commercial-off-the-shelf
DDS	Data Dissemination Service
DIL	Disconnected Operations, Intermittent Connectivity, Limited Communications
DISR	DoD Information Technology Standards Registry
DoD	Department of Defense
GNEC	Global Network Enterprise Construct
IA	Information Assurance
IDE	Integrated Development Environment
IdM	Identity Management
IPN	Installation Processing Node
IT	Information Technology
ME	Mission Environments
NEC	Network Enterprise Center
PASS	Publish and Subscribe Services
RACE	Rapid Access Computing Environment
SDK	Software Development Kit

Acronyms	
Acronym	**Description**
TDY	Temporary Duty
TRL	Technology Readiness Level
TRM	Technical Reference Model
USMC	United States Marine Corps
OSs	Operating Systems