



JOINT REQUIREMENTS
OVERSIGHT COUNCIL

THE JOINT STAFF
WASHINGTON, D.C. 20318-8000

JROCM 173-07
16 July 2007

MEMORANDUM FOR DISTRIBUTION

Subject: Net-Enabled Command Capability Increment One Capability
Development Document

1. The Joint Requirements Oversight Council (JROC) approves the Net-Enabled Command Capability (NECC) Increment **One Capability** Development Document and Extensions, and validates the **enclosed** key performance parameters and key system attributes. The JROC will **maintain** approval authority for all key performance parameter changes, **delegates** capability development document approval authority oversight for **changes to key system attributes** to the Joint Capabilities Board, and **delegates** capability development document approval authority for all other non-key performance parameter/non-key system attribute changes to USJFCOM via the **Joint Combat Capability Developer** organization as outlined in the capability development document. Capability developers will use the NECC Capability Development Document and Extensions as the initial statement of validated capability needs for all phases of development. This program is assigned the Joint Potential Designator of "JROC Interest."
2. USJFCOM, working in concert with the Services and appropriate agencies, will determine program funding requirements for POM 2010 and beyond.
3. Should the Defense Information Systems Agency encounter costs exceeding ten percent of the approved acquisition program baseline or 25 percent of the original program baseline (Program Acquisition Unit Cost/Acquisition Procurement Unit Cost), they shall **return** to the JROC prior to reprogramming or budgeting additional funding into the program.
4. The JROC recognizes the importance of the NECC program and requests USJFCOM return to the JROC to provide annual program updates.


E. P. GIAMBASTIANI
Admiral, US Navy
Vice Chairman
of the Joint Chiefs of Staff

Enclosure

UNCLASSIFIED // FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY



**Net-Enabled Command Capability (NECC)
Capability Development Document (CDD)
Linked Extension C - Glossary**

Increment: I

7 June 2007

This document has been approved by J8 for release to
Australia, Canada, and Great Britain

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Table Of Contents

GLOSSARY..... C-1

Foreign Releaseability

This document is authorized for release (either hardcopy or electronically) to Australia, Canada, and Great Britain governments and their respective contractors and representatives working as mutual defense cooperative capability partners in support of NECC.

AUS, CAN, GBR government agencies and their defense support contractors may disseminate “For Official Use Only” information to their employees and subcontractors who have a need for the information. Removal of the “For Official Use Only” marking can only be accomplished by the USJFCOM J88. All “For Official Use Only” information shall be stored in locked receptacles such as file cabinets, desks, or bookcases. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection. During working hours, the information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. Transmission of “For Official Use Only” information may only be accomplished on a government-to-government basis.

Further requests for this document should be submitted to:

Joint Combat Capability Developer (J88)
U.S. Joint Forces Command
1562 Mitscher Avenue, Suite 200
Norfolk, Virginia 23551-2488

Points of Contact

John Wellman, NECC JCCD Lead, J88 USJFCOM, (757) 836-0126, john.wellman@jfc.com

John Costello, NECC Washington Liaison Office Lead, J882DC USJFCOM, (703) 614-5016, john.costello@jfc.com

John Nankervis, NECC Capability Development & DOTMLPF Lead, J882B USJFCOM, (757) 836-6310, john.nankervis@jfc.com

Extension C – Glossary

PART I – ABBREVIATIONS AND ACRONYMS

A

A2C2S	Army Airborne Command and Control System
AADC	Area Air Defense Commander
AAR	After Action Report
ABCS	Army Battle Command System
ACAT	Acquisition Category
ACP	Airspace Control Point
ACP	Allied Communications Publication
ACO	Air Combat Order
ACO	Airspace Control Order
ACTD	Advanced Concept Technology Demonstration
ADatP	Allied Data Publications
ADC	Air Defense Commander
ADNS	Automated Digital Network System
ADP	Air Defense Plan
AES	Advanced Encryption Standard
AFC2ISRC	Air Force Command and Control & Intelligence, Surveillance, and Reconnaissance Center
AFDD	Air Force Doctrine Document
AFFOR	Air Force Forces
AH	Authorization Header
AI	Artificial Intelligence
AIS	Automated Information System
AITI	Automated Interchange of Technical Information
AML	Additional Military Layers
AMP	Air Mobility Plan
ANSI	American National Standards Institute
AO	Area of Operation
AoA	Analysis of Alternatives
AOC	Air and Space Operations Center
AOR	Area Of Responsibility
AP	Adaptive Planning
APD	Advance Planning Document
APEX	Adaptive Planning and Execution
API	Application Program Interface
APPG	Annual Planning and Programming Guidance
AREC	Air Resource Element Coordinator
ARFOR	Army Forces
ASCC	Army Service Component Command
ASD	Assistant Secretary of the Defense
ASOCC	Area Security Operations Command and Control System
ASR	Air Support Request
ASUW	Anti-Surface Warfare
ASW	Anti-Submarine Warfare
AT&L	Acquisition Technology & Logistics
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order

UNCLASSIFIED // FOR OFFICIAL USE ONLY

NECC Capability Development Document Extensions – Version 1.0

7 June 2007

AV Architectural View or All View

B

BA Battlespace Awareness
BAS Battlefield Automation Systems
BC Battle Command
BCOTM Battle Command On The Move
BDA Battle Damage Assessment
BE Basic Encyclopedia
BEA Business Enterprise Architecture
BFT Blue Force Tracking
BLOS Beyond Line of Sight
BM Battle Management
BRD Baseline Requirements Document
BUFR Binary Unit Format Representation

C

C Celsius
C2 Command and Control
C2W Command and Control Warfare
C4I Command, Control, Communications, Computers, and Intelligence
C4IM C4 and Information Management
C4ISR Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAE Component Acquisition Executive
CALS Communications Area Local Station
CAOC Combined Air Operations Center
CAPP Controlled Access Protection Profile
CAS Close Air Support
CBEFF Common Biometric Exchange File Format
CBRNE Chemical, Biological, Radiological, Nuclear, and High Explosives
CCDR Combatant Commander
CCIC2S Combatant Commanders Integrated Command and Control System
CCIR Commander's Critical Information Requirements
CCP Common Computing Platform
CDD Capabilities Development Document
CDR Commander
CDS Cross Domain Solution
CE Controlled Extensions
CENTRIXS Combined Enterprise Regional Information Exchange System
CES Core Enterprise Services
CESP Civil Engineering Support Plan
CFACC Combined Forces Air Component Commander
CGI Computer Graphics Interface
CI Capability Interface
CIA Central Intelligence Agency
CID Combat Identification
CIM Common Information Model
CINC Commander in Chief
CIO Chief Information Officer
CIP Critical Infrastructure Protection
CIPG Cryptographic Interface Programmers Guide
CJCS Chairman of the Joint Chiefs of Staff
CJCSI Chairman of the Joint Chiefs of Staff Instruction

UNCLASSIFIED // FOR OFFICIAL USE ONLY

NECC Capability Development Document Extensions – Version 1.0

7 June 2007

CJCSM	Chairman of the Joint Chiefs of Staff Manual
CJFLCC	Coalition Joint Force Land Component Commander
C/JMTK	Commercial / Joint Mapping Tool Kit
CM	Collection Management
CM	Consequence Management
CN	Capability Needs
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COA	Course of Action
COCOM	Combatant Command (Command Authority)
COE	Common Operating Environment
CoE	Center of Excellence
COI	Community of Interest
COMAFFOR	Commander, Air Force Forces
COMINT	Communications Intelligence
COMSEC	Communications Security
CONOPS	Concept of Operations
CONPLAN	Concept Plan
CONUS	Continental United States
COP	Common Operational Picture
COTS	Commercial off-the-shelf
CPD	Capabilities Production Document
CPG	Contingency Planning Guidance
CR	Crisis Response
CR/CM	Crisis Response / Consequence Management
CRD	Capabilities Requirement Document
CSA	Chief of Staff of the Army
CSAR	Combat Search and Rescue
CSG	Carrier Strike Group
CTC	Combined Training Centers
CTL	Candidate Target List
CTP	Common Tactical Picture

D

D&D	Denial and Deception
DAA	Designated Approving Authority
DAB	Defense Acquisition Board
DBMS	Database Management System
DCID	Director of Central Intelligence Directive
DCIO	Deputy Chief Information Officer
DCGS	Distributed Common Ground/Surface System
DCGS-A	Distributed Common Ground/Surface System – Army
DCMA	Defense Contracts Management Agency
DCP	Deployable Command Post
DCTS	Defense Collaborative Tool Set
DDMS	Defense Discovery Metadata Standards
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIACAP	Defense Information Assurance Certification and Accreditation Process
DICAST	Defense Intelligence Communication Accreditation Support Team
DICOM	Digital Imaging and Communications in Medicine
DII	Defense Information Infrastructure

C-3

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

DIME	Diplomatic, Information, Military, Economic
DIRLAUTH	Direct Liaison Authorized
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DOD Information Technology Standards Registry
DJC2	Deployable Joint Command and Control
DLA	Defense Logistics Agency
DMI	Desktop Management Interface
DMPI	Designated Mean Point of Impact
DMS	Defense Message System
DNC	Digital Nautical Charts
DNS	Domain Name Server
DOD	Department of Defense
DODAF	Depart of Defense Architectural Framework
DODD	DOD Directive
DODI	DOD Instruction
DODIIS	DOD Intelligence Information System
DOE	Department of Energy
DOJ	Department of Justice
DOM	Document Object Model
DOS	Department of State
DOT	Department of Transportation
DOTMLPF	Doctrine, Organization, Training, Material, Leadership and Education, Personnel, and Facilities
DPG	Defense Planning Guidance
DPI	Desired Point of Impact
DR	Disaster Relief
DRSN	Defense RED Switched Network
DSA	Digital Signal Algorithm
DSN	Defense Switched Network
DSS	Digital Signature Standard
DTO	Daily Tasking Order
DTRA	Defense Threat Reduction Agency
DTS	Defense Transportation System
DTSS	Digital Topographic Support System
DVS-G	DISN Video Services – Global

E

E3	Electromagnetic Environment Effects
E3SM	Electromagnetic Environment Effects and Spectrum Management
EAS	Evolutionary Acquisition Strategy
EBO	Effects Based Operations
EBP	Effects Based Planning
ECL	EMW Capabilities List
ECS	Environmental Control Services
ECU	Environmental Control Unit
EDI	Electronic Data Interchange
EDIFACT	EDI For Administration, Commerce and Transport
EI	Essential Elements of Information
EFR	Equipment Facilities Requirements
EIE	Enterprise Interface Environment
ELINT	Electronic Intelligence
ELRR	Expeditionary Long Range Radar
EMC	Electro-Magnetic Compatibility

UNCLASSIFIED // FOR OFFICIAL USE ONLY

NECC Capability Development Document Extensions – Version 1.0

7 June 2007

EMP	Electromagnetic Pulse
EMPRS	Enroute Mission Planning & Rehearsal System
EMW	Expeditionary Maneuver Warfare
EPIP	Evolutionary Phased Implementation Plan Availability
EPW	Enemy Prisoners of War
ESG	Expeditionary Strike Group
ESP	Encapsulating Security Protocol
EW	Electronic Warfare

F

4D	Four Dimension (X, Y, Z, Time)
F	Fahrenheit
FBI	Federal Bureau of Investigation
FCD	Final Committee Draft
FC-PH	Fiber Channel - Physical Signaling Interface
FCS	Future Combat System
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research & Development Center
FIO	Foreign Influence Operations
FIPS	Federal Information Processing Standards
FLTCDR	Fleet Commander
FM	Field Manual
FOC	Full Operational Capability
FoS	Family of Systems
FOUO	For Official Use Only
FRAGO	Fragmentary Order
FSCL	Fire Support Coordination Line
FTP	File Transfer Protocol
FUNCPLAN	Functional Plan
FY	Fiscal Year
FYDP	Fiscal Year Defense Plan

G

GBM	Global Ballistic Missile
GCCS	Global Command and Control System
GCCS-A	Global Command and Control System – Army
GCCS-AF	Global Command and Control System – Air Force
GCCS-J	Global Command and Control System – Joint
GCCS-M	Global Command and Control System – Maritime
GCSS	Global Combat Support System
GES	Global Information Grid - Enterprise Services
GEOINT	Geospatial Intelligence
GFM	Global Force Management
GIF	Graphic Interchange Format
GIG	Global Information Grid
G/M	Grams per Meter
GMD	Ground Missile Defense
GMI	General Military Intelligence
GOTS	Government off the Shelf
GPS	Global Positioning System
GRIB	Gridded Binary
GriD	GCCS Requirements Database
GSORTS	Global Status of Resources and Training System
GTN	Global Transportation Network

C-5

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

NECC Capability Development Document Extensions – Version 1.0

7 June 2007

GUI Graphical User Interface
GWOT Global War On Terror

H

HA Humanitarian Assistance
HAE Height Above Ellipsoid
HCI Human-Computer Interface
HD Homeland Defense
HDBT Hardened, Deeply Buried Targets
HDF Hierarchal Data Format
HERO Hazards of Electromagnetic Radiation to Ordnance
HF High Frequency
HFDL High Frequency Data Link
HGI Human-GIG Interface
HHQ Higher Head Quarters
HMI Human Machine Interface
HPT High Performance Team
HQ Headquarters
HQDA Headquarters, Department of the Army
HMAC Keyed-Hashing for Message Authentication
HS Homeland Security
HSI Human Systems Integration
HSOC Home Station Operations Center
HTML Hyper Text Markup Language
HTTP Hyper Text Transfer Protocol
HUMINT Human Intelligence

I

I&RTS Integration and Run Time Specification
IA Information Assurance
IAC Inter-Agency Community
IAMD Integrated Air and Missile Defense
IAVA Information Assurance & Vulnerability Assessment
IAW In Accordance With
IC Intelligence Community
ICAO International Civil Aviation Organization
ICD Initial Capabilities Document
ICD Intelligence Community Directive
IC MAP Intelligence Community Multi-Intelligence Acquisition Program
ICTO Interim Certification To Operate
ID Identification
IDM Information Dissemination Management
IDS Intrusion Detection System
IEEE Institute of Electrical and Electronics Engineers
IER Information Exchange Requirement
IETF Internet Engineering Task Force
IEW Improved Early Warning
IFF Identification, Friend or Foe
IFR Instrument Flight Rules
IKE Internet Key Exchange
IMOM Improved Many-on-Many
INCITS International Committee for Information Technology Standards
IN/HR Inches per Hour

UNCLASSIFIED // FOR OFFICIAL USE ONLY

IO	Information Operations
IOC	Initial Operational Capability
IOS	Intelligence and Operations Server
IP	Internet Protocol
IPB	Intelligence Preparation of the Battlespace
IRIG	Inertial Reference Integrating Gyro
ISAKMP	Internet Security Association and Key Management Protocol
ISBN	International Standard Book Number
ISBT	Integrated Science Business and Technology
ISEA	In-Service Engineering Activity Warehouse Facility
ISMA	Internet Streaming Media Alliance
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISP	Information Support Plan
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
ITU	International Telecommunication Union
ITU-R	ITU - Radiocommunication Sector
ITU-T	ITU - Telecommunication Standardization Sector
IW	Information Warfare
IWL	Interoperability Watch List

J

JAEC	Joint Assessment and Enabling Capability
JAOP	Joint Air Operations Plan
JBMC2	Joint Battle Management Command and Control
JC2	Joint Command and Control
JCAPS	Joint C4ISR Architecture Planning/Analysis System
JCAS	Joint Close Air Support
JCB	Joint Capabilities Board
JCCD	Joint Combat Capability Developer
JCD	Joint Capabilities Document
JCIDS	Joint Capability Integration and Development System
JCS	Joint Chiefs of Staff
JDL	Joint Directors of Laboratories
JDN	Joint Data Network
JDS	Joint Deployment System
JDST	Joint Decision Support Tools
JEMPRS-NT	Joint Enroute Mission Planning & Rehearsal System – Near Term
JFACC	Joint Force Air & Space Component Commander
JFAST	Joint Flow and Analysis System for Transportation
JFC	Joint Force Commander
JFCOM	Joint Forces Command
JFC	Joint Functional Concept
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
JFP	Joint Force Provider
JFSOA	Joint Forces Space Operations Authority
JIADS	Joint Integrated Air defense System
JIM	Joint, Interagency, and Multi-national
JIPB	Joint Intelligence Preparation of the Battlefield
JIPCL	Joint Integrated Prioritized Collection List
JIPTL	Joint Integrated Prioritized Target List
JITC	Joint Interoperability Test Command

UNCLASSIFIED // FOR OFFICIAL USE ONLY

JKDDC	Joint Knowledge Development and Distribution Capability
JMAST	Joint Mobile Ashore Support Terminal
JMCIS	Joint Maritime Command and Control System
JMEM	Joint Munitions Effectiveness Manual
JNMS	Joint Network Management System
JNTC	Joint National Training Capability
JOA	Joint Operational Architecture
JOC	Joint Operations Center
JOPEs	Joint Operation Planning and Execution System
JOpsC	Joint Operations Concepts
JP	Joint Publication
JPEC	Joint Planning and Execution Community
JPD	Joint Potential Designator
JPEG	Joint Photographic Experts Group
JPEO	Joint Program Executive Office
JPO	Joint Program Office
JRD3C	Joint Rapid Distributed Database Development Capability
JROC	Joint Requirements Oversight Council
JROCM	JROC Memorandum
JS	Joint Staff
JS/C/S/A	Joint Staff/Combatant Commander/Service/Agency
JSCP	Joint Strategic Capabilities Plan
JSOC	Joint Special Operations Command
JSOTF	Joint Special Operations Task Force
JSPS	Joint Strategic Planning System
JSTRAP	Joint System Training Plan
JTF	Joint Task Force
JTFC	Joint Training Functional Concept
JTGE	Joint Training Global Environment
JTF HQ	Joint Task Force Headquarters
JTRS	Joint Tactical Radio System
JTT	Joint Targeting Toolbox
JWARN	Joint Warning and Reporting Network
JWICS	Joint Worldwide Intelligence Communications System
JWID	Joint Warfighter Interoperability Demonstration

K

KC	Knowledge Center
KEA	Key Exchange Algorithm
KIP	Key Interface Profile
KM	Knowledge Management
KPP	Key Performance Parameter
KSA	Key System Attribute

L

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LD-CELP	Low-Delay Code Excited Linear Prediction
LMS	LAN Management System
LOAC	Law of Armed Conflict
LOC	Lines of Communication
LOM	Learning Objective Metadata
LOS	Line of Sight
LRU	Lowest Replaceable Unit

UNCLASSIFIED // FOR OFFICIAL USE ONLY

NECC Capability Development Document Extensions – Version 1.0

7 June 2007

LSPP	Labeled Security Protection Profile
LT	Language Translation
LTSA	Learning Technology Systems Architecture
LW	Land Warrior

M

\$M	Millions of Dollars
M&S	Modeling and Simulation
MAC	Medium Access Control
MAGTF	Marine Air-Ground Task Force
MA ICD	Mission Area Initial Capabilities Document
MAIS	Major Automated Information System
MARFOR	Marine Forces
MASINT	Measurement and Signature Intelligence
MCDP	Marine Corps Doctrinal Publication
MCP	Mission Capability Package
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MEF	Marine Expeditionary Force
MELP	Mixed Excitation Linear Prediction
METOC	Meteorological and Oceanographic
MGCP	Media Gateway Control Protocol
MGR	Military Grid Reference
MHS	Message Handling System
MICFAC	Mobile Integrated Command Facilities
MIDB	Modernized Intelligence Database
MILHDBK	Military Handbook
MIL-PRFs	Defense Performance Standards
MILSATCOM	Military Satellite Communications
MIL-STDs	Military Standards
MIN	Minute
MIOC	Maritime Intercept Operation Commander
MISREP	Mission Report
MIUW	Mobile Inshore Undersea Warfare
MIW	Mine Warfare
MIWC	Mine Warfare Commander
MLS	Multi-Level Security
MNG	Multiple-image Network Graphics
MNIS	Multinational Information Sharing
MNS	Mission Needs Statement
MOCC	Mobile Operational Command Center
MOE	Measures of Effectiveness
MOOTW	Military Operations Other Than War
MOPP	Mission Oriented Protective Posture
MPA	Maritime Patrol Aircraft
MOSA	Modular Open Systems Architecture
MP-CDL	Multi-platform Common Data Link
m/s	Meters per Second
MS	Milestone
MSC	Major Subordinate Command
MSL	Multiple Security Levels
MTI	Moving Target Indicator
MTM	Module Test and Maintenance
MTP	Mission Training Plan

C-9

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

N

N/A	Not Applicable
NAIC	National Air and Space Intelligence Center
NATO	North Atlantic Treaty Organization
NAVEUR	Naval Forces Europe
NAVFOR	Naval Forces
NAVICP	Naval Inventory Control Point
NAVOCEANO	Naval Oceanographic Office
NBC	Nuclear, Biological, Chemical
NCCA	Naval Center for Cost Analysis
NCDS	Net-Centric Data Strategy
NCES	Network Centric Enterprise Services
NCOW	Net-Centric Operations and Warfare
NCOW RM	NCOW Reference Model
NDI	Non-Developmental Items
NEC	Net-Enabled Capability
NECC	Net-Enabled Command Capability
NET	New Equipment Training
NETOPS	Network Operations
NETWARS	Network Warfare Simulation
NGA	National Geospatial-Intelligence Agency
NGO	Non-Governmental Organization
NIAP	National Information Assurance Partnership
NIE	National Intelligence Estimate
NII	Networks and Information Integration
NIPRNet	Non-Secure Internet Protocol Network
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NLOS	Non-Line of Sight
NMCI	Navy – Marine Corps Intranet
NMCS	National Military Command System
NR-KPP	Net-Ready Key Performance Parameter
NRO	National Reconnaissance Office
NRT	Near Real Time
NSA	National Security Agency
NSANET	National Security Agency Network
NSC	National Security Council
NSCS	National Security Council System
NSS	National Security Systems
NTCS-A	Navy Tactical Command System – Afloat
NWF	Networked Fires

O

O&M	Operations and Maintenance
OASD	Office of the Assistant Secretary of Defense
OCONUS	Outside the Continental United States
OE	Operating Environment
OIF	Operation Iraqi Freedom
OLB	Object Language Bindings
OMG	Object Management Group
OMN	Operations and Maintenance, Navy
ONA	Operational Net Assessment
ONI	Office of Naval Intelligence

UNCLASSIFIED // FOR OFFICIAL USE ONLY

NECC Capability Development Document Extensions – Version 1.0

7 June 2007

OoB	Order of Battle
OPLAN	Operation Plan
OPN	Other Procurement, Navy
OPNAV	Naval Operations
OPORD	Operation Order
OPSEC	Operations Security
OPTES	Overall, Personnel, Training, Equipment, Supplies
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OSINT	Open Source Intelligence
OSPF	Open Shortest Path First
OUSD	Office of the Under Secretary of Defense
OV	Operational View

P

PASV	Passive
PBA	Predictive Battlespace Awareness
PCI	Peripheral Component Intercomponent
PCM	Pulse Code Modulation
PDF	Portable Document Format
PEO C4I	Program Execution Office C4I
PERSTEMPO	Personnel Tempo of Operations
PESQ	Perceptual Evaluation of Speech Quality
PHY	Physical Layer
PIF	Pseudonym Identification Feature
PIN	Personal Increment Number
PIR	Priority Intelligence Requirements
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PMESII	Political, Military, Economic, Social, Infrastructure and Information
PMI	Prevention of Mutual Interference
PMW	Program Manager - Warfare
PNG	Portable Networks Graphics
POL	Petroleum, Oil, and Lubricants
POM	Program Objective Memorandum
PoR	Program of Record
POSIX	Portable Operating System Interface
POTUS	President of the United States
PPBES	Planning, Programming, Budgeting, and Execution System
PSE	Peculiar Support Equipment
PSM	Packet Switch Model
PTDO	Prepare to Deploy Order
PUMA	Persistent Unmanned Multi-role Aircraft

Q

QDR	Quadrennial Defense Review
QoS	Quality of Service

R

RADIUS	Remote Authorized Dial In User Service
RCC	Regional Combatant Commander
RDT&E	Research, Development, Test, and Evaluation
RF	Radio Frequency
RFA	Radio Frequency Authorization

UNCLASSIFIED // FOR OFFICIAL USE ONLY

RFC	Request For Comments
RFC	Request for Capability
RFF	Request for Forces
RFI	Request for Information
RFT	Ready for Training
RGS	Requirements Generation System
RID	Requirements Identification Document
RM	Reference Model
ROE	Rules of Engagement
ROMO	Range of Military Operations
RT	Real Time

S

S	Secret
SA	Situational Awareness
SABI	Secret and Below Interoperability
SAFE	Selected Area for Evasion
SAP	Special Access Programs
SARPS	Surveillance Radar and Collision Avoidance System
SATS	Standard Architecture for Testing Systems
SC	Space Control
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facilities
SCORM	Sharable Content Object Reference Model
SDN	Secure Data Network
SECDEF	Secretary of Defense
SECOMP-I	Secure En route Communications Package - Improved
SGML	Standard Generalized Markup Language
SIAP	Single Integrated Air Picture
SIF	Selective Identification Feature
SIGINT	Signals Intelligence
SIPRNet	Secret Internet Protocol Router Network
SISSU	Secure, Interoperable, Supportable, Sustainable, and Usable
SITREP	Situational Report
SJFHQ	Standing Joint Force Headquarters
SLA	Service Level Agreement
SLATE	System Level Automation Tool for Engineers
SME	Subject Matter Expert
SMI	Structure of Management Information
SMT	Scar, Mark and Tattoo
S/NF	Secret / No Foreign
SNMP	System Network Management Protocol
SOA	Service Oriented Architectures
SOAP	Simple Object Access Protocol
SOF	Special Operations Forces
SOP	Standard Operating Procedures
SoS	System of Systems
SOSO	Stability Operations and Support Operations
SPAWAR	Space and Naval Warfare Systems Command
SQL	Structured Query Language
SSC	Smaller-Scale Contingencies
SSL	Secure Sockets Layer
STANAGs	NATO Standardization Agreements
STAR	System Threat Assessment Report

UNCLASSIFIED // FOR OFFICIAL USE ONLY

NECC Capability Development Document Extensions – Version 1.0

7 June 2007

STEP	Standardized Tactical Entry Point
STO	Space Tasking Order
STOU	Store Unique
STRIKE	Software for Targeting Requirements information Operations and Kinetic Effects
STT	Submarine Tactical Terminal
STWC	Strike Warfare Commander
SUS	Single UNIX Specification
SUWC	Surface Warfare Commander
SV	System View
SVC	Service
SWC	Undersea Warfare Commander
SWOSCOM	Surface Warfare Officers' School Command

T

2D	Two Dimension (X,Y)
3D	Three dimension (X, Y, Z)
3DESE	Triple Data-Encryption Standard Encryption Protocol
T2	Training Transformation
T2IP	Training Transformation Implementation Plan (T2IP)
TABI	Top Secret and Below Interoperability
TAC	Tactical Air Coordinator
TACAN	Tactical Air Navigation
TACC	Tactical Air Control Center
TACOPDAT	Tactical Operations Data Message
TACSAT	Tactical Satellite
TAMD	Theater Air and Missile Defense
TARGET	Theatre-level Analysis, Replanning, and Graphical Extension Toolbox
TBD	To Be Determined
TBM	Theater Ballistic Missile
TBMCS	Theater Battle Management Core System
TC	Target Correlation
TC-AIMS	Transportation Coordinators' Automated Information for Movement System
TCAS	Traffic Alert and Collision Avoidance System
TCN	Transportation Control Number
TCP/IP	Transmission Control Protocol / Internet Protocol
TDL	Tactical Data Link
TED	Threat Environment Description
TELNET	Telephone Network
TEMP	Test and Evaluation Master Plan
TES	Theatre Event System
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TMDE	Test, Measurement, Diagnostic, Equipment
TNL	Target Nomination List
TOC	Tactical Operations Center
TOD	Tactical Ocean Data
TP	TRADOC Publication
TPED	Tasking, Processing, Exploitation, and Dissemination
TPFDD	Time-Phased Force and Deployment Data
TPPU	Task, Post, Process, Use
TRADOC	Training and Doctrine Command
TS	Top Secret
TSA	Target System Analysis
TSABI	Top Secret/SCI And Below Interoperability

C-13

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

NECC Capability Development Document Extensions – Version 1.0

7 June 2007

TSC	Tactical Support Center
TSIG	Transaction Signature
TST	Time Sensitive Targets
TTE	Technical Test & Evaluation
TTG	Tactical Training Group
TTP	Tactics, Techniques and Procedures
TV	Technical View
TWG	Technology Work Group

U

U	Unclassified
UA	Unit of Action
UAV	Unmanned Aerial Vehicle
UCP	Unified Command Plan
UCS	Universal Multiple-Octet Coded Character Set
UGV	Unmanned Ground Vehicles
UIC	Unit Identification Code
UID	Unit Identification
UJTL	Universal Joint Task List
ULN	Unit Line Numbers
µm	Microns
URI	Universal Resource Identifier
URL	Uniform Resource Locator
URL	Universal Record Locator
US	United States
USA	United States Army
USAF	United States Air Force
USCENTCOM	US Central Command
USD	Under Secretary of Defense
USEUCOM	US European Command
USJFCOM	US Joint Forces Command
USMC	United States Marine Corps
USMTF	US Message Text Format
USN	United States Navy
USNAVCENT	US Naval Central Command
USNORTHCOM	US Northern Command
USPACOM	US Pacific Command
USSOCOM	US Special Operations Command
USSOUTHCOM	US Southern Command
USSTRATCOM	US Strategic Command
USTRANSCOM	US Transportation Command
USW	Under Sea Warfare
UTC	Unit Type Code
UTM	Universal Transverse Mercator

V

VACM	View-based Access Control Model
VKB	Virtual Knowledge Base
VME	Virtual Machine Environment
VPF	Vector Product Format
VPN	Virtual Private Network
VTC	Video Teleconferencing
VXI	VME bus Extensions for Instrumentation

W

WARM	Wartime Reserve Mode
WGS	World Geodetic System
WIN-T	Warfighter Information Network - Tactical
WMD	Weapons of Mass Destruction
WMO	Web Management Option
WSDL	Web Services Description Language
WSM	Water-space Management
WSTAWG	Weapons System Technical Architecture Working Group

XYZ

XHTML	Extensible HTML
XMI	XML Metadata Interchange
XML	Extensible Markup Language
XPATH	XML Path Language
XSL	Extensible Stylesheet Language

PART II – DEFINITIONS

Access. A specific type of interaction between a subject (i.e., a person, process, or input device) and an object (i.e., an automated information system resource such as a record, file, program, or output device) resulting in the transfer of information. The ability and opportunity to obtain knowledge of classified, sensitive or unclassified information.

Accreditation. The process by which an IT and NSS are evaluated for meeting security requirements to maintain the security of both the information and the information systems. A designated accreditation authority (DAA) is named for each system. Co-DAAs accredit IT and NSS in certain cases involving interoperability or integration of multiple systems.

Acquisition Category (ACAT). Categories established to facilitate decentralized decision making as well as execution and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures. DOD 5000.2-R, Part 1, provides the specific definition for each acquisition category (ACAT I through III).

ACAT I. A major defense acquisition program (MDAP) subject to Defense Acquisition Board oversight and estimated by the USD (AT&L) to require an eventual total expenditure of more than \$355 million in RDT&E funds, or \$2.135 billion in procurement funds measured in FY 1996 constant dollars.

ACAT IA. A major automated information system (MAIS) acquisition program estimated to require program costs in any single year in excess of \$30 million, total program costs in excess of \$120 million, or total life cycle costs in excess of \$360 million (FY 1996 constant dollars).

ACAT IAC. A major automated information system acquisition program for which the DOD chief information officer (CIO) has delegated milestone decision authority (MDA) to the

component acquisition executive (CAE) or component CIO. The “C” (in ACAT IAC) refers to component.

ACAT IAM. A major automated information system (MAIS) acquisition program for which the MDA is the DOD CIO.

ACAT IC. A major defense acquisition program subject for which the MDA is the DOD component head, or if delegated, the DOD component acquisition executive (CAE). The “C” refers to component.

ACAT ID. MDAP for which the MDA is USD (AT&L). The “D” refers to the Defense Acquisition Board (DAB), which advises the USD(AT&L) at major decision points.

Adaptive Planning. Adaptive Planning (AP) is the Joint capability to create and revise plans rapidly and systematically, as circumstances require. AP occurs in a networked, collaborative environment, requires the regular involvement of senior DOD leaders, and results in plans containing a range of viable options.

At full maturity, AP will form the backbone of a future joint adaptive planning and execution system, supporting the development and execution of plans. AP will preserve the best characteristics of present day deliberate and crisis planning with a common process. (AP Roadmap, 13 December 2005)

Advanced Concept Technology Demonstration (ACTD). A demonstration of the military utility of a significant new capability and an assessment to clearly establish operational utility and system integrity.

Agency. For purposes of this document, the term Agency refers to the following IC agencies of [Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), Service Intelligence Centers and Activities, and National Security Agency (NSA)], and the following DOD agencies [e.g. Defense Information Systems Agency (DISA), Defense Logistics Agency (DLA), Defense Threat Reduction Agency (DTRA), Defense Contracts Management Agency (DCMA)].

Alliance. The result of formal agreements (i.e. treaties) between two or more nations for broad, long-term objectives that further the common interests of the members (JP-1-02). For the purpose of NECC requirements, Allies regularly integrate operations on a national, organizational, and/or individual basis; and have significant functional capabilities that support interoperability.

All Views (AV). There are some overarching aspects of architecture relating to all three of the views. These overarching aspects are captured in the All Views (AV) products. The AV products provide information pertinent to the entire architecture, but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture. The scope includes the subject area and timeframe for the architecture. The setting in which the architecture exists comprises the interrelated conditions composing the context for the

architecture. These conditions include doctrine; tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions.

Analysis of Alternatives (AoA). The evaluation of the operational effectiveness, operational suitability and estimated costs of alternative systems to meet a mission capability. The analysis assesses the advantages and disadvantages of alternatives being considered to satisfy capabilities, including the sensitivity of each alternative to possible changes in key assumptions or variables.

Architecture. The structure, relationships, principles and guidelines governing component design and evolution.

Attribute. A testable or measurable characteristic describing an aspect of a system or capability.

Automated Information System (AIS). A combination of computer hardware and computer software, data, and/or telecommunications performing functions such as collecting, processing, storing, transmitting and displaying information. Excluded are computer resources, both hardware and software, that are: physically part of, or dedicated to, or essential in real time to the mission performance of weapons systems; used for weapon system specialized training, simulation, diagnostic test and maintenance, or calibration; or used for research and development of weapon systems.

Battle Management. The art of translating battlespace information into effective combat action. Battle management is the exercise of "decentralized execution." It is that part of command and control not involving the exercise of command authority and includes controlling and directing the application of force. It also includes decisions and actions taken in indirect response to the enemy actions and decisions and actions taken while controlling and directing executions of commander's intent and while translating operational-level orders into tactical delegation of targets. Battle management is the subordination of execution to command authority and therefore, can occur at strategic, operational and tactical levels of war depending on the commander's operational domain. (CONOPS for C2 Constellation)

Battlespace. The environment, factors, and conditions which must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest. (JCS Pub 1-02)

Battlespace Awareness. The ability of the Joint Force Commander to understand the operational environment and the adversary. To ensure DOD can dissuade, deter, and defeat threats to the Homeland, the Joint Force Commander should have a comprehensive understanding of the battlespace (within the limits set by law), including the capability to detect the full range of threats – conventional and unconventional – enabled through an interlocking field of sensors with deep reach and remote surveillance capability fused with national-level intelligence collection and analysis to provide common situational awareness across the spectrum of

participants for all domains in the operating environment (air, space, land, maritime, and cyber). (Source: BA JFC)

Capability. The ability to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms in the format of an initial capabilities document or a DOTMLPF change recommendation. In the case of material proposals, the definition progressively evolves to DOTMLPF performance attributes identified in the CDD and the CPD.

Capability Development Document (CDD). A document capturing the information necessary to develop a proposed program(s), normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable, and technically mature capability.

Capability Gaps. Those synergistic resources (DOTMLPF) unavailable but potentially attainable to the operational user for effective task execution.

Capability Production Document (CPD). A document addressing the production elements specific to a single increment of an acquisition program.

Capstone Requirements Document (CRD). A document containing capabilities-based requirements facilitating the development of CDDs and CPDs by providing a common framework and operational concept to guide their development. Per JROCM 095-04, all CRDs are being converted to Joint Capabilities Documents (JCD) (formerly Mission Area Initial Capabilities Documents (MA ICD)).

Center of Excellence (CoE). Public institutions (e.g., universities, Federally Funded Research and Development Centers (FFRDCs), non-profit organizations) providing subject matter expertise, data, and other analytical services and support relevant to joint interagency and/or multinational operations.

Certification. A statement of adequacy provided by a responsible agency for a specific area of concern supporting the validation process. Certification consists of three forms of capability confirmation -- first, one addresses system interoperability requirements; second, one addresses supportability; and third, one addresses total life-cycle oversight of warfighter interoperability requirements. The two J-6 certifications and validation are discussed below.

a. J-6 Developmental and Production Capabilities Interoperability Certification. This certification occurs prior to each acquisition milestone (B, C). The J-6 certifies ORDs, CDDs, CPDs and ISPs regardless of ACAT level, for conformance with joint IT and NSS policy and doctrine and interoperability standards. As part of the review process, J-6 requests assessments from the Services, OSD, DISA and DOD agencies.

b. J-6 Supportability Certification. The J-6 certifies to OASD (NII) that programs, regardless of ACAT, adequately address IT and NSS infrastructure requirements, the availability of bandwidth and spectrum support, funding, and personnel, while also identifying dependencies and interface requirements between systems. As part of the review process, J-6 requests

UNCLASSIFIED // FOR OFFICIAL USE ONLY

supportability assessments from DISA and DOD agencies. J-6 conducts a supportability certification for CPD, prior to Milestone C for submission to OASD (NII) as part of the CPD review process.

c. J-6 Interoperability System Validation. The J-6 validation is intended to provide total life cycle oversight of warfighter capabilities interoperability. The J-6 validates the DISA (JITC) interoperability system test certification, which is based upon a joint certified NR-KPP, approved in the CDD, CPD and ISP. The validation occurs after receipt and analysis of the DISA (JITC) interoperability system test certification. The J-6 issues an interoperability system certification memorandum to the respective Services, agencies, and developmental and operational testing organizations.

Coalition. An ad hoc arrangement between two or more nations for common action (JP 1-02)

Coalition Interface. Any interface passing information between one or more US IT and NSS and one or more coalition partner IT and NSS.

Collaborative Environment. An environment utilizing a suite of fully integrated, web-enabled applications for a virtual aggregation of individuals and organizations, communications pathways, infrastructure, and procedures to create and share the data, information, and knowledge needed to plan, execute, and assess joint force operations and to enable a commander to make decisions better and faster than the adversary. (Also referred to as the collaborative information environment)

Combat Power. Combat power is the combination of a unit's physical and moral capabilities and the interaction between the two. It can be tailored to a specific mission and be estimated by quantifying physical items, such as combat vehicles for example and their associated kit such as fuel and ammunition, combined with moral strength such as morale and available quality of leadership enabled by quality of information IAW the health of the network. These sums and interactions can be calculated based on commander guidance to achieve an approximation of combat power that the commander can temper with his judgment and experience. The list below establishes the kinds of information that contribute to calculation and estimate of combat power but is not comprehensive.

Leadership. The cohesion of units and the presence and effectiveness of trained, competent and locally aware leaders establishes the limits of potential unit missions and probability for success.

Replenishment. The capability for commander and staff to see and anticipate losses, monitor consumption, and automatically generate replenishment to a predetermined level based on operating tempo and battlefield mission requirements.

Network Status. The current and projected status of the network for capacity, speed, accuracy, information management, reach, etc., to determine the degree to which the commander and unit can prosecute information based operations and tie together the moral and physical components of unit combat power.

Command and Control (C2). The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JCS Pub 1-02)

Commercial-Off-The-Shelf (COTS). Refers to an item of hardware or software produced by a contractor and is available for general purchase. Such items are at the unit level or higher. Such items must have been sold and delivered to government or commercial customers, must have passed customer's acceptance testing, and must be operating under the customer's control and within the user environment. Further, such items must have meaningful reliability, maintainability, and logistics historical data. (TAFIM 2.0, vol. 1)

Common Operating Environment (COE). The COE is an integrated software infrastructure, which facilitates the migration and implementation of functional mission applications and integrated databases across information systems.

Automation services supporting the development of the common reusable software modules that enable interoperability across multiple combat support applications. This includes segmentation of common software modules from existing applications, integration of commercial products, development of a common architecture, and development of common tools for application developers. Also called COE. (JCS Pub 1-02)

Common Operational Picture (COP). For NECC, a COP is the aggregate collection of information required to present a decision maker or group of decision makers with all relevant information needed to understand the interrelationships of current BLUE/RED/GRAY air and space operations, land operations, and maritime operations through a mission-relevant set of battlespace visualizations.

The common operational picture is a distributed data processing and exchange environment for developing a dynamic database of objects, allowing each user to filter and contribute to this database, according to the user's area of responsibility and command role. The common operational picture provides the integrated capability to receive, correlate, and display a common tactical picture, including planning applications and theater-generated overlays and projections (i.e., environmental, battle plans, force position projections). Overlays and projections may include location of friendly, hostile, and neutral units, assets, and reference points. The common operational picture may include information relevant to the tactical and strategic level of command. This includes, but is not limited to, any geographically oriented data, planning data from Joint Operation Planning and Execution System, readiness data from Global Status of Resources and Training System, intelligence (including imagery overlays), reconnaissance data, environmental (air, land, sea, and space), predictions of nuclear, biological, and chemical fallout, and air tasking order data. (CJCSI 3151.01A)

A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. (JCS Pub 1-02)

Common Tactical Picture (CTP). An accurate and complete display of relevant tactical data, supporting a joint task force integrating tactical information from the multi-tactical data link network, composite tracking network, intelligence network, and ground digital network. The common tactical picture enables command and control, situational awareness, and combat identification, as well as supporting the tactical elements of all joint mission areas. The common tactical picture, along with information from the joint planning network, contributes to the common operational picture. The common tactical picture is derived from sensor information and other sources and refers to the current depiction of the battlespace for a single operation within a combatant commander's area of responsibility. This responsibility includes current, anticipated or projected, and planned disposition of hostile, neutral, and friendly forces as they pertain to US [joint] and multinational operations ranging from peacetime through crisis and war. The CTP includes force location, real time and non-real time sensor information, and amplifying information. Also called CTP. (CJCSI 3151.01A)

Communities of Interest (COI). Collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have shared vocabulary for the information they exchange. (DCIO DOD Net-Centric Data Strategy, dated 9 May 2003)

Computer resources. Components physically part of, dedicated to, or essential in real time to mission performance used for weapon system specialized training, simulation, diagnostic test and maintenance or calibration; or used for research and development of weapon systems.

Configuration Management. A discipline applying technical and administrative direction and surveillance to: (1) identify and document the functional and physical characteristics of a configuration item; (2) control changes to those characteristics; and (3) record and report changes to processing and implementation status. (JCS Pub 1-02)

Connectivity. The ability to exchange information by electronic means. (JCS Pub 1-02)

The comprehensive linking of command, control, communications and computer (C4) systems establishes a level of connectivity which enables communication to and from the joint force and its users. To the maximum extent possible, the hardware and software interfaces should be transparent to the system user. The continued flow of information should not depend on action by an intermediate user. (JCS Pub 6-02)

Contingency Planning Guidance (CPG). Provides guidance to the combatant commanders concerning contingencies and includes the Prioritized Regional Objectives for DOD. The CPG emphasizes theater-wide vice country-specific planning, a revised set of planning factors, and the integration of conventional military planning with nuclear planning and non-military instruments of national power.

Contingency Sourcing. The process of identifying backfill/substitute forces for plans when forces previously identified are not operationally available on a specified date.

Core Enterprise Services (CES). A collection of networked capabilities enabling DOD service providers. The CESs provide and manage the underlying capabilities to deliver content and value to end-users, and are currently binned into nine capability groups: Enterprise Service Management, Messaging, Application, Discovery, Mediation, Collaboration, Storage, Information Assurance / Security, and User Assistance. All CES capabilities, except Enterprise Service Management and User Assistance, correlate directly to NECC's Cross-Functions.

Critical IER. An information exchange that is so significant that if it does not occur the mission area is adversely impacted (CJCSI 6212.01B).

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (JCS Pub 1-02)

Database Management System. A computer application program which accesses or manipulates the database. [HCI Style Guide] Defense Information Infrastructure (DII) – A seamless web of communications networks, computers, software, databases, applications, and other capabilities meeting the information processing and transport needs of DOD users in peacetime and crises operations.

Data Interoperability. Interoperable – Many-to-many exchanges of data occur between systems, through interfaces that are sometimes predefined or sometimes unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed. Data administration is intended to promote interoperability through standardization of data elements, minimize duplication of data elements across the Department, and reduce the need for data element translation. (DOD Data Strategy, 9 May 2003 and DODD 8320.2-G, 7 Nov 2005).

Data Standardization. Developers will be responsible for adhering to published net-centric interoperability standards, including data standards where applicable. Successful discovery and interoperability of data assets depend on compliance with metadata standards in the DOD Metadata Registry and the DISR [i.e., Defense Discovery Metadata Standards (DDMS)] and data exposure standards found in the DOD Service Registry (e.g., GES discovery interface standards). For example, data assets that are maintained by the Department's Records management functions must provide a means for the Enterprise discovery capability to query the inventory of their stored records. In doing so, these records management applications should employ DDMS to respond to Enterprise discovery queries. (DOD Data Strategy, 9 May 2003 and DODD 8320.2-G, 7 Nov 2005).

Defense-in-Depth. The citing of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver the reserve. (JCS Pub 1-02)

Defense Information Infrastructure (DII). The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving the Department of Defense (DOD) local, national, and worldwide information needs. The defense information infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. (JCS Pub 1-02)

Defense Transportation System (DTS). The portion of the Nation's transportation infrastructure that supports Department of Defense common-user transportation needs across the range of military operations. It consists of those common-user military and commercial assets, services, and systems organic to, contracted for, or controlled by the Department of Defense.

Department of Defense (DOD) Agencies. For purposes of this document DOD Agencies include the combat support agencies [e.g. Defense Information Systems Agency (DISA), Defense Logistics Agency (DLA), Defense Threat Reduction Agency (DTRA), Defense Contracts Management Agency (DCMA)]. Note: This document also applies to information and data sharing with non-DOD agencies such as the Department of Homeland Security (HS/HD) to include the US Coast Guard, White House Office of Homeland Security, and Federal Bureau of Investigation (FBI).

Deployable Joint Command and Control system (DJC2). The DJC2 system will provide Regional Combatant Commanders (RCCs) with an integrated, rapidly deployable Joint C2 capability specifically tailored to support the Joint Force Commander (JFC) in executing Standing Joint Force Headquarters (SJFHQ) and Joint Task Force Headquarters (JTF HQ) operations. The system will consist of a suite of C2 applications; data systems; hardware; networking components; supporting infrastructure (shelters, power, etc.); mobility components; and limited organic en route and early entry communications capabilities. DJC2 will be modularized to be capable of different configurations for deployment packages to meet varying RCC C2 requirements.

Designated Approving Authority (DAA). The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement recording the decision to accept those safeguards. The DAA must be at an organizational level, have authority to evaluate the overall mission requirements of the AIS, and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS. (DODD 8500.1)

Domain Values. Provides acceptable values associated with attributes (characteristics) of Entities (Database Objects/Subjects). Example: A field for gender may have the domain {male, female, unknown} where those three values are the only permitted entries.

Dual Tasking. A unit is apportioned to a plan and sourced to an event in progress on C Day and the number of personnel required in the plan plus the number of personnel required in the event

exceeds the Unit Assigned Strength or the quantity of equipment required in the plan plus the quantity of equipment required in the event exceeds Unit Assigned Equipment. When a unit is dual tasked contingency sourcing is required.

Effect. The physical and/or behavioral state of a system that results from an action, a set of actions or another effect.

Effects Based Approach to Operations. A process for obtaining a desired strategic outcome or "effect" on the enemy, through the synergistic, multiplicative, and cumulative application of the full range of military and nonmilitary capabilities at the tactical, operational, and strategic levels.

Effects Based Approach to Joint Operations. An enhancement to the current planning process that emphasizes consideration of the various effects (physical and / or behavioral changes in the state of a system) caused by an action or a set of actions that result from application of capabilities associated with the instruments of national power (diplomatic, informational, military, and economic). (JWFC Commanders Handbook for an Effects-based approach to Joint Operations).

Effects Based Assessment (EBA). Assessing the various effects (physical and/or behavioral changes in the state of a system) caused by an action or set of actions that result from application of capabilities associated with the instruments of national power (diplomatic, informational, military, and economic).

Effects Based Planning (EBP). EBP is an operational planning process conducted within the request for a deployment order process. EBP is results-based vice attrition-based. EBP closely mirrors the current joint planning process, yet focuses upon the linkage of actions to effects to objectives. EBP changes the way we view the enemy and ourselves, and what is included and emphasized in the planning process. EBP uses a flexibly structured battle rhythm that leverages a collaborative knowledge environment and capitalizes on the use of fewer formal joint boards. It employs virtual, near-simultaneous planning at all echelons of command.

Electromagnetic compatibility (EMC). The ability of systems, equipment and devices using the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation response. It involves the application of sound electromagnetic Spectrum Supportability; system, equipment, and device design configuration ensuring interference-free operation; and clear concepts and doctrines that maximize operational effectiveness. (JCS Pub 1-02)

Electromagnetic Environmental Effects (E3). E3 is the impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including compatibility, interference; vulnerability, pulse; protection; hazards of radiation to personnel, ordnance, and volatile materials; and natural phenomena effects, of lightning and precipitation static. (JCS Pub 1-02)

Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. **Source: DODI 8500.2, 6 February, 2003 Para E2.1.17.2.**

Environment. In the context of the COE, all software running from the time the computer is rebooted to the time the system is ready to respond to operator queries after login. This software includes the operating system, security software, installation software, windowing environment, COE services, etc. The environment is subdivided into a runtime environment and a software development environment.

Evolutionary Acquisition. DOD's preferred strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in increments, recognizing up-front the need for future capability improvements.

Family-of-Systems (FoS). A set or arrangement of independent systems arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation. (Defense Acquisition Guidebook V1.0, 17 Oct 2004)

Force Employment. Transition from force-level planning to execution including C2 activities associated with management of assets.

Force Generation. Bring forces to a state of readiness for operations by recruiting, assembling and organizing personnel, supplies and materiel. This includes the training and equipping of forces and the provision of means for deployment, sustainment and recovery. It also embraces catering to concurrent operations, recuperation, mobilization and reconstitution.

Force Projection. The ability to project the military element of national power from the continental United States (CONUS) or another theater, in response to requirements for military operations. Force projection operations extend from mobilization and deployment of forces to redeployment to CONUS or home theater. (JCS Pub 1-02)

Force Protection. Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. (JCS Pub 1-02)

Force Readiness (Readiness). The ability of US military forces to fight and meet the demands of the national military strategy. Readiness is the synthesis of two distinct but interrelated levels.

a. unit readiness--The ability to provide capabilities required by the combatant commanders to execute their assigned missions. This is derived from the ability of each unit to deliver the outputs for which it was designed. b. joint readiness--The combatant commander's ability to integrate and synchronize ready combat and support forces to execute his or her assigned missions. (JCS Pub 1-02)

Force Sustainment (Sustainment). The provision of personnel, logistic, and other support required to maintain and prolong operations or combat until successful accomplishment or revision of the mission or of the national objective. (JCS Pub 1-02)

Full Operational Capability (FOC). A CDD will describe the types and quantities of assets required to attain full operational capability. FOC identifies operational units [CCDRs for NECC] (including other Services or government agencies, if appropriate) that will employ the capability, and defines the asset quantities (including spares, training, and support equipment, if appropriate) required. (CJCSM 3170.01B)

Global Combat Support System (GCSS). A management framework providing responsive, flexible, and effective management visibility of cross-functional, cross-service, and multi-echelon activities, (e.g., logistics, manpower, and finance) with the purpose of supporting operational mission accomplishment by the commander.

Global Command and Control System (GCCS) Family of Systems (FoS). GCCS-Joint and Service variants to include GCCS-A, GCCS-AF, GCCS-M, GCCS-K, and GCCS-I3.

Global Force Management (GFM). Process to align force apportionment, assignment, and allocation methodologies in support of the National Defense Strategy and joint force availability requirements; present comprehensive visibility of the global availability and operational readiness of U.S, conventional military forces; globally source joint force requirements; and provide senior decision makers a vehicle to quickly and accurately assess the impact and risk of proposed allocation, assignment and apportionment changes. (SECDEF Memo OSD 78395-04 of 4 May 2005)

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security Systems, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and

deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems. (JCS Pub 1-02)

Global Information Grid (GIG) Enterprise Services (ES). The approach to providing the GIG infrastructure needed for timely, secure, ubiquitous edge user access to decision quality information. [OASD (NII)] A collection of net-based capabilities for use in the DOD enterprise, the GES is composed of the networks, core services, and community services combined.

Global Transportation Network (GTN). GTN is the automated support necessary to enable USTRANSCOM and its components to provide global transportation management. It provides the integrated transportation data and systems necessary to accomplish global transportation planning, command and control, and in-transit visibility across the range of military operations. The designated DOD in-transit visibility system provides customers with the ability to track the identity, status, and location of DOD units and non-unit cargo, passengers, patients, forces, and military and commercial airlift, sealift, and surface assets from origin to destination across the range of military operations. The GTN collects, integrates, and distributes transportation information to combatant commanders, Services, and other DOD customers. GTN provides USTRANSCOM with the ability to perform C2 operations, planning and analysis, and business operations in tailoring customer requirements throughout the requirements process.

Homeland Defense — The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President. The Department of Defense is responsible for homeland defense. Homeland defense includes missions such as domestic air defense. The Department recognizes that threats planned or inspired by “external” actors may materialize internally. The reference to “external threats” does not limit where or how attacks could be planned and executed. The Department is prepared to conduct homeland defense missions whenever the President, exercising his constitutional authority as Commander in Chief, authorizes military actions. Also called **HD**. (JP 3-26)

Homeland Security — Homeland security, as defined in the National Strategy for Homeland Security, is a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. The Department of Defense contributes to homeland security through its military missions overseas, homeland defense, and support to civil authorities. Also called **HS**. (JP 3-26)

Homeland Security/Homeland Defense (HS/HD) components. For purposes of this document, HS/HD components include the Department of Homeland Security, White House Office of Homeland Security, and Federal Bureau of Investigation (FBI).

Humanitarian Assistance (HA) - Assistance to the local populace provided by predominantly US forces in conjunction with military operations and exercises. This assistance is specifically authorized by title 10, United States Code, section 401, and funded under separate authorities. Assistance provided under these provisions is limited to (1) medical, dental, and veterinary care provided in rural areas of a country; (2) construction of rudimentary surface transportation

systems; (3) well drilling and construction of basic sanitation facilities; and (4) rudimentary construction and repair of public facilities. Assistance must fulfill unit training requirements that incidentally create humanitarian benefit to the local populace.

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JCS Pub 3-13)

Information Exchange Requirements (IER). Information exchange requirements characterize the information exchanges to be performed by the proposed system(s). For CDDs, top-level IERs are information exchanges between systems of combatant command/Service/agency, allied, and coalition partners. For CPDs, top-level IERS are information exchanges external to the system (i.e., with other combatant commands/Services/Agencies, allied and coalition systems). IERs identify who exchanges what information with whom, why the information is necessary, and how the information exchange must occur. Top-level IERs identify warfighter information used supporting a particular mission-related task and exchanged between at least two operational systems supporting a joint or combined mission. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the IER.

Information Support Plan (ISP). Used by program authorities to document the IT and NSS needs, objectives, and interface requirements for all ACAT and non-ACAT and fielded programs. ISPs should be kept current throughout the acquisition process and formally reviewed at each milestone, decision reviews, and whenever the operational concepts and IT and NSS support requirements change.

Information Technology (IT). Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Information technology does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

Initial Capabilities Document (ICD). A document identifying the need for a materiel solution to a specific capability gap derived from an initial analysis of alternatives executed by the operational user and, as required, an independent analysis of alternatives. It defines the capability gap by functional area, relevant range of military operations, desired effects, and time.

Integrated Architecture. An architecture consisting of multiple views or perspectives (Operational View, Systems View, and Technical Standards View), facilitating integration and promoting interoperability across family of systems and system of systems and compatibility among related architectures. An architecture description has integrated Operational, Systems, and Technical Standards Views with common points of reference linking the Operational View

to the Systems View and the Systems View to the Technical Standards View. An architecture description is defined to be an *integrated architecture* when products and their constituent architecture data elements are developed to ensure architecture data elements defined in one view are the same (i.e., same names, definitions, and values) as those referenced in another view.

Intelligence. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Also, information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (USJFCOM Glossary)

Intelligence certification. Confirmation by Joint Staff J2 IRCO of the availability, suitability, and sufficiency of intelligence to support a system or program. Intelligence certification also provides: (1) an assessment of the impact of a system or program on joint intelligence strategy, policy, architectural planning, and needs of the warfighter and (2) an evaluation of open systems architectures, interoperability, and compatibility for intelligence handling and intelligence-related information systems. This certification occurs as a prerequisite for the system acquisition process and at each acquisition milestones.

Intelligence Community (IC). For purposes of this document, the IC is comprised of the Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), Service Intelligence Centers and Activities, and the National Security Agency (NSA).

Interagency Community (IAC). As based on the 2003 Handbook Management for Complex Crisis Handbook, Appendix D, the IAC includes the Departments of State (DOS), Defense (DOD), Transportation (DOT), Justice (DOJ), and Energy (DOE), along with the Central Intelligence Agency (CIA), Department of Homeland Security, Treasury Department, Federal Emergency Management Agency (FEMA), White House Office of Homeland Security, and National Security Council (NSC).

Interim Certificate to Operate (ICTO). Authority to field new systems or capabilities for a limited time, with a limited number of platforms, to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an ICTO is made by the MCEB Interoperability Test Panel based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.

Interoperability. a. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together, and b. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them or their users. The degree of interoperability should be defined when referring to specific cases. For the purposes of this instruction, the degree of interoperability is determined by the accomplishment of the proposed IER fields. (JCS Pub 1-02)

Interoperability Watch List (IWL). Established by the USD (AT&L), the ASD (NII)/DOD CIO, Director Operational Test & Evaluation, the Chairman of the Joint Chiefs of Staff, and the Commander, U.S. Joint Forces Command, to provide DOD oversight for those IT and NSS activities for which interoperability issues deemed critical to mission effectiveness are not being adequately addressed. IT and NSS considered for the IWL may be pre-acquisition systems, acquisition programs (any ACAT), already fielded systems, or combatant commander-unique procurements.

Joint. Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (JCS Pub 3-13)

Joint C4ISR Architecture Planning/Analysis System (JCAPS). DOD-approved static architecture tool for manipulating and conducting analysis of operational and systems architectures.

Joint Capabilities Board (JCB). The JCB functions to assist the JROC in carrying out its duties and responsibilities. The JCB reviews and, if appropriate, endorses all JCIDS and DOTMLPF proposals prior to submission to the JROC. The Joint Staff, J-8, Director of Force Structure, Resources, and Assessment is the JCB chair. It is comprised of Flag Officer / General Officer representatives of the Services.

Joint Data Network (JDN). Outlines Joint Data Network operations in a CJTF. Establishes the JDN as a rapidly deployable, responsive and scaleable information management capability that provides accurate decision quality data to ensure positive command and control during each critical phase of JTF operations. JDN is composed of the Multi-Tactical Data Link Network, Sensor Network, Ground Network and Intelligence Network. Defines the roles and responsibilities of the Joint Data Network Operations Officer (JDNO) in producing the Common Tactical Picture as well as the Joint Interface Control Officer (JICO).”

Joint Functional Concepts (JFCs). An articulation of how a future joint force commander will integrate a set of related military tasks to attain capabilities required across the range of military operations. Although broadly described within the Joint Operations Concepts, they derive specific context from the Joint Operating Concepts and promote common attributes in sufficient detail to conduct experimentation and measure effectiveness.

Joint Integrated Architecture. An integrated architecture establishing the basis for rapidly acquiring affordable and evolving joint warfighting capabilities through collaborative planning, analysis, assessment, and decision making.

Joint Interface. An IT and NSS interface passing or used to pass information between systems and equipment operated by two or more combatant commanders, Services, or Agencies.

Joint Interoperability Testing and Certification. The process of assessing the ability of a system to exchange usable electronic information with systems of other services or nations as specified in its requirements documents. Specialized test tools monitor performance of products

to determine if proper actions and reactions are produced. A system is certified as interoperable at the completion of successful interoperability testing.

Joint National Training Capability (JNTC). A collection of interoperable training sites, nodes, and events that synthesizes Combatant Commander and Service training requirements and enables trainers to provide the appropriate “joint context.” Founded upon the four pillars of (1) realistic combat training, (2) an adaptive and credible opposing force, (3) common ground truth, and (4) high quality feedback, the JNTC is a global, information age capability that advances Defense Department transformation efforts enabling multinational, interagency, and intergovernmental training - from tactical through strategic levels - in a spectrum of live, virtual and constructive training environments. **(Reference: Management Initiative Decision (MID) 906, January 2003).**

Joint Operating Concept (JOC). An articulation of how a future joint force commander will plan, prepare, deploy, employ, and sustain a joint force against potential adversaries’ capabilities or crisis situations specified within the range of military operations. Joint Operating Concepts guide the development and integration of JFCs to provide joint capabilities. They articulate the measurable detail needed to conduct experimentation and allow decision makers to compare alternatives.

Joint Operations Planning and Execution System (JOPES). The system providing the foundation for conventional command and control by national- and combatant command-level commanders and their staffs. It is designed to satisfy their information needs in the conduct of joint planning and operations. Joint Operations Planning and Execution System (JOPES) includes joint operation planning policies, procedures, and reporting structures supported by communications and automated data processing systems. JOPES is used to monitor, plan, and execute mobilization, deployment, employment, sustainment, and redeployment activities associated with joint operations. (JCS Pub 1-02)

Joint Operations Concepts (JOpsC). A concept describing how the Joint Force intends to operate 15 to 20 years in the future. It provides the operational context for the transformation of the Armed Forces of the United States by linking strategic guidance with the integrated application of Joint Force capabilities.

Joint Planning and Execution Community (JPEC). Headquarters, commands, and agencies involved in the training, preparation, movement, reception, employment, support, and sustainment of military forces assigned or committed to a theater of operations or objective area. It usually consists of the Joint Staff, Services (including major commands), Combatant Commands (and Service components), Joint Task Forces, Defense Logistics Agency, and other Defense Agencies as applicable to a given scenario. (JCS Pub 1-02)

Joint Potential Designator (JPD). A designation assigned by the Gatekeeper to specify JCIDS validation, approval, and interoperability expectations.

a. “JROC Interest” designation applies to all ACAT I/IA programs and programs designated as JROC Interest. This designation may also apply to intelligence capabilities supporting DOD and national intelligence requirements. These documents are staffed through the JROC for validation and approval. All Mission Area ICDs/CRDs are designated as JROC Interest. DOTMLPF change proposals also are designated as JROC Interest.

b. “Joint Impact” designation applies to ACAT II-and-below programs where the concepts and/or systems associated with the document affect the joint force such that an expanded review is appropriate to ensure the most appropriate and effective solution is developed for the joint warfighter. This designation also applies to intelligence capabilities supporting both national intelligence and DOD not designated as JROC Interest. A Functional Capabilities Board validates Joint Impact proposals, returning them to the sponsor for approval and acquisition.

c. “Joint Integration” designation applies to ACAT II and below programs where the concepts and/or systems associated with the document do not significantly affect the joint force and an expanded review is not required. However, National Security Systems and Information Technology Systems (NSS and ITS) interoperability, intelligence or munitions certification is required. Once the required certification(s) are completed, Joint Integration proposals are validated and approved by the sponsoring component.

d. “Independent” designation applies to ACAT II and below programs where the concepts and/or systems associated with the document do not significantly affect the joint force, an expanded review is not required, and no certifications are required. Once designated, these documents are returned to the sponsoring component for validation and approval.

Joint Requirements Oversight Council Memorandum (JROCM). Official JROC correspondence generally directed to an audience(s) external to the JROC. JROCMs are usually decisional in nature.

JROC special interest. Programs identified by the JROC Secretary as being of interest to the JROC for oversight even though they do not meet the ACAT I cost thresholds or have been designated as ACAT ID.

Joint System Training Plan (JSTRAP). The preferred training method used to take advantage of efficiencies available with a common approach to training. Training plans address number and type of personnel to be trained, training concept, and training solution to be used. A training solution should be determined through a Job Task Analysis, Training Task Analysis, Media Analysis, and Cost Analysis, and be sufficiently detailed to describe the training resources required (e.g., time to train, facilities, instructors, equipment, etc.)

Joint Task Force (JTF). A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. (JCS Pub 1-02)

Key Interface. Interfaces in functional and physical characteristics, existing at a common boundary, with co-functioning items, systems, equipment, software, and data. They are designated as a Key Interface when one or more of the following criteria are met:

- a. The interface spans organizational boundaries. Different entities (service, agency, organization) have ownership and authority over the hardware and software capabilities on either side of the boundary,
- b. The interface is mission critical. Data from joint organizations, multiple services, and/or multiple agencies/organizations must move across the interface to satisfy joint information flow requirements. If systems are not interoperable at that interface, the ability to accomplish the mission is endangered.
- c. The interface is difficult or complex to manage.
- d. There are capability, interoperability, or efficiency issues associated with the interface.
- e. The interface impacts multiple acquisition programs, usually more than two (e.g. network points of presence, many-to-many or one-to-many connections).
- f. The interface is vulnerable or important from a security perspective.

Key Interface Profile (KIP). An operational functionality, systems functionality, and technical specifications description of the Key Interface. The profile consists of refined Operational and Systems Views, Interface Control Document/Specifications, Engineering Management Plan, Configuration Management Plan, Technical View with SV-TV Bridge, and Procedures for Standards Conformance and Interoperability Testing.

Key Performance Parameters (KPPs). Those capabilities or characteristics considered essential for successful mission accomplishment. Failure to meet a system or program's KPP threshold can cause the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a system or program's KPP threshold can cause family-of-systems or system-of-systems concepts to be reassessed or the contributions of the individual systems to be reassessed. KPPs are validated by the JROC. KPPs are included in the acquisition program baseline.

Key System Attribute (KSA). An attribute or characteristic considered crucial in support of achieving a balanced solution/approach to a key performance parameter (KPP) or some other key performance attribute deemed necessary by the sponsor. KSAs provide decision makers with an additional level of capability performance characteristics below the KPP level and require a sponsor 4-star, Defense agency commander, or Principal Staff Assistant to change. (CJCSI 3170.01)

Knowledge Management (KM). 1) The management of knowledge—applying the principles of management to the generation, codification, storage, distribution, and re-use of knowledge. KM attempts to make conscious the processes that humans employ and to update those processes with modern technology and psychology. People generally learn consciously and explicitly, either through personal experience or from other people. KM attempts to build upon the former to enhance the latter, so as to create a more cost-effective knowledge organization. In parallel,

unconscious, tacit knowledge is generally learned personally (through intuition, hunches, attunements) or collectively (through one's culture, rituals, ceremonies, and shared experiences of a less-defined nature).

2) The process for effectively applying intellectual capital (human, social, and organizational) to enable faster, better organizational decisions. Tools, such as decision support systems, can provide content to decision makers faster and more coherently but cannot actually effect decision making by themselves. KM can be viewed as an interface or cusp between human psychology and process and (information) technology, though it has been characterized as two-thirds human and one-third technology (at most). (Know-IT Encyclopedia, September 2002)

Levels of Fusion. The levels of fusion as described by the Joint Directors of Laboratories are:

- 1) Multi-target tracking and attribute fusion (identification)
- 2) Automated reasoning for situation assessment
- 3) Development of alternate hypothesis for threat assessment
- 4) Monitoring and control of fusion processes

Levels of Processing. The levels of processing as described by the Joint Directors of Laboratories are:

- 1) Denotes the conversion of sensor data into a reference frame
- 2) Denotes the current relationship among objects for interpretation within a scene
- 3) Estimates the future from the current situation with a combative strategy
- 4) Monitors the fusion process and identifies the sensory information required for inferencing

Metadata Catalogues. The DOD Metadata Registry, based on the International Organization for Standardization (ISO) 11179 specification for metadata registries, is available throughout the Enterprise (GES). The Registry represents a “onestop shop for developer data needs” and is a key component in achieving the Department's interoperability goals. All document formats, interface definitions, and exchange models used by systems will be stored in the DOD Metadata Registry. Developers can discover these metadata assets and utilize them to read, write, or exchange data that is made available throughout the Enterprise. All programs and COIs have a responsibility to support interoperability through active participation in the DOD Metadata Registry. The DOD Metadata Registry will provided capabilities to further support interoperability through the use of translation and mediation services and for the sharing and reuse of processes. (DOD Data Strategy, 9 May 2003)

Milestone Decision Authority (MDA). The individual designated in accordance with criteria established by the USD (AT&L), or by the ASD (NII) for acquisition programs, to approve entry of an acquisition program into the next phase.

Milestones. Major decision points separating the phases of an acquisition program.

Mission Area Initial Capability Document (MA ICD). A document designed to be the next step in ensuring capabilities contributing to specific mission areas complies with the standards and KPPs necessary for the successful completion of the mission. MA ICDs are converted CRDs as directed by JROCM 095-04.

Mission Capability Package (MCP). NECC MCPs are DOTMLPF capabilities binned together to form readily identifiable capability sets to facilitate support of the warfighter via evolutionary acquisition and incremental fielding of capability improvement(s). Each MCP is supported by Service/Agency-provided software applications developed and organized to meet joint capability mission area and warfare domain-specific execution requirements. The currently identified and supported NECC Program MCPs include: Force Projection, Force Readiness, Intelligence, Situational Awareness, Force Employment - Air/Space Operations, Force Employment – Land Operations, Force Employment – Maritime/Littoral Operations, and Force Protection.

Mission Need. A deficiency in current capabilities or an opportunity to provide new capabilities (or enhance existing capabilities) through the use of new technologies. They are expressed in broad operational terms by the DOD components.

Mission Needs Statement (MNS). A formatted non-system specific statement containing operational capability needs, written in broad operational terms. It describes required operational capabilities and constraints to be studied during the Concept Exploration and Definition Phase of the Requirements Generation Process. (JCS Pub 3-13).

Mission Partners. All partners engaged in a unified action where achieving mission objectives require integration of joint force actions with agencies, non-governmental organizations, first responders, tribal and private volunteer organizations CONUS and OCONUS.

Multi-Level Security (MLS). Capability for a system (e.g. workstation, server, network, or combination) to store data at multiple classifications (e.g. S, TS, TS/SCI), to provide access to users who are not cleared for all stored data, and to control access to the stored data and services based on pre-defined rules.

Multi-National. Between two or more forces or agencies of two or more nations or coalition partners (JP 1-02). For the purposes of NECC requirements “multi-national” is further defined to include joint forces, non-governmental organizations, first responders, tribal and private volunteer organizations CONUS and OUTCONUS.

Multiple Security Levels (MSL). An architecture in which systems, data and users on disparate classification levels are fully segregated, except for specific interconnection points. Data exchange at the interconnection points is managed by guarding systems.

National Military Command System (NMCS). The NMCS is the priority command component utilizing NECC to support the President, Secretary of Defense and the Joint Chiefs of Staff in exercising their military command responsibilities. It includes the National Airborne Operations Center, the Alternate National Military Command Center, the National Emergency Airborne Command Post, and other command centers designated by the Secretary of Defense. It

also includes the communications connecting those command centers with the headquarters of the combatant commanders, Services, and other commands and agencies who support joint operation planning via NECC. The NMCS also provides coordination with activities outside the Department of Defense [e.g., the White House Situation Room and the Central Intelligence Agency (CIA) Operations Center] that have operation planning and execution functions. The Chairman of the Joint Chiefs of Staff is responsible to the Secretary of Defense for operating the NMCS to meet the needs of the President and the Secretary of Defense.

National Security Systems (NSS). Telecommunications and information systems operated by the Department of Defense, the functions, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves the command and control of military forces; (4) involves equipment integral to a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications).

Near Real Time (NRT).

a. Pertaining to the timeliness of data or information that has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JCS Pub 1-02)

b. Data or information delayed by the time required for electronic communication and automatic data processing. Data is older than real time due to data processing, but does not impact the current planning cycle – no significant delays. (CJCSI 3151.01)

Net-Centricity. Net-centricity enables user access and use of resources both collaboratively and asynchronously, regardless of time and place. It is the ability of a program or system to integrate with, offer services to, and exploit the services of a net-centric environment.

Net Centric. Exploitation of advancing technology moving from an applications-centric to a data-centric paradigm - that is, providing users the ability to access applications and services through Web services, an information environment comprised of interoperable computing and communication components.

Net-Centric Enterprise Services (NCES). A DISA program to implement key enabling capabilities for a net-centric enterprise. NCES provide a common set of interoperable information capabilities in the Global Information Grid (GIG) to access, collect, process, store, disseminate, and manage information on demand for warfighters, policy makers, and support organizations.

Net Centric Operations and Warfare (NCOW). Describes how DOD conducts business operations, warfare, and enterprise management. It is based on the concept of an assured, dynamic, and shared information environment providing access to trusted information for all users, based on need, independent of time and place. It is characterized by assured services,

infrastructure transparency (to the user), independence of data consumers and producers, and metadata supported by information discovery, protection and mediation. This fundamental shift from platform-centric to net-centric warfare provides for an Information Superiority-enabled concept of operations. The NCOW RM provides a common taxonomy and lexicon of NCOW concepts and terms and architectural descriptions of NCOW concepts. It represents an important mechanism in DOD transformation efforts, establishing a common framework for net-centricity. It enables capability developers, program managers, and program oversight groups to move forward on a path toward a transformed, net-centric enterprise.

Net Centric Operations and Warfare Reference Model (NCOW RM). The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities [core services, Community of Interest (COI) services, and environment control services], and the enterprise management components. It also describes a selected set of key standards needed as the NCOW capabilities of the Global Information Grid (GIG) are realized. The NCOW RM represents the objective end-state for the GIG. This objective end-state is a service-oriented, inter-networked, information infrastructure in which users request and receive services enabling operational capabilities across the range of military operations; DOD business operations; and Department-wide enterprise management operations. The NCOW RM is a key compliance mechanism for evaluating DOD information technology capabilities and the Net Ready Key Performance Parameter.

Net-Enabled Command Capability (NECC). Beginning in the FY08-10 timeframe, NECC replaces GCCS-J and Service variants as the DOD principal command and control information technology. The objective “mission space” for this capability is defined as the area supporting command capability and C2 activities from the National Military Command System (NMCS) through the Joint Task Force (JTF) and Service/Functional components to unit level commanders. NECC integrates existing and emerging C2 capabilities through an enterprise-based joint architecture integrating applications and databases forming to support Joint warfighters, coalition partners, and agencies responsible for homeland security and defense. NECC is a systems integrator, not an equipment system, developed holistically along with parallel improvements in DOT_LPF. NECC provides agile C2 capability allowing joint forces to operate within the adversary's decision cycle by facilitating enhanced battlespace awareness, timely information exchange, and net-centric information sharing to support critical joint and multinational operations.

Network Centric Warfare. An information superiority-enabled concept of operations generating increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher operations tempo, greater lethality, increased survivability, and a degree of self-synchronization. Network centric warfare translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

Net-Ready. DOD IT/NSS meeting required information needs, information timeliness requirements, has information assurance accreditation, and meets the attributes required for the

technical exchange of information and the end-to-end operational effectiveness of that exchange. DOD IT/NSS which is Net-Ready, enables warfighters and DOD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure, leveraging service modularity, multimedia connectivity, metadata, and collaboration to provide an environment promoting unifying actions among all participants. Net-readiness requires IT/NSS to operate in an environment where there exists a distributed information processing environment in which applications are integrated; applications and data independent of hardware are integrated and information transfer capabilities exist to ensure seamless communications within and across diverse media. Additionally, information is in a common format with a common meaning; there is a common human-computer interface for users; and effective means to protect the information exists. Net-Readiness is critical to achieving the envisioned objective of a cost-effective, seamlessly integrated environment. Achieving and maintaining this vision requires interoperability:

- a. Within a Joint Task Force/combatant command area of responsibility (AOR).
- b. Across combatant command AOR boundaries.
- c. Between strategic and tactical systems.
- d. Within and across Services and Agencies.
- e. From the battlefield to the sustaining base.
- f. Among US, Allied, and Coalition forces.
- g. Across current and future systems.

Net-Ready Key Performance Parameter (NR-KPP). The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of the exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements: a. Compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM), b. Compliance with applicable GIG Key Interface Profiles (KIPs), c. Verification of compliance with DOD information assurance requirements, and d. Supporting integrated architecture products required to assess information exchange and use for a given capability.

Net-Ready KPP Assessment. The Net-Ready KPP Assessment determines the impacts, risks, and vulnerabilities of fielding secure, interoperable, supportable, sustainable and usable (SISSU) systems to the warfighter. Parameters assessed include: network security, network impact, compatibility with the infrastructure, infrastructure requirements, spectrum support, security policy compliance, DISR standards compliance, communications and information manpower, training, logistics support, schedule, and funding. A system assessed and determined to be supportable from a communications and information perspective is considered Net Ready when any impacts, risks and vulnerabilities it may present to the enterprise are deemed to be acceptable or manageable.

Network warfare simulation (NETWARS). The standard DOD approved communications simulation tool. Combatant commanders, Services and Agencies use NETWARS for all communications modeling purposes.

Non-Acquisition (Non-ACAT) Program. An effort not directly resulting in the purchase of a system or equipment for operational employment (e.g., science and technology programs, concept exploration or advanced development of potential acquisition programs).

Open System. A system which implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (1) to be ported with minimal changes across a wide range of systems, (2) to interoperate with other applications on local and remote systems, and (3) to interact with users in a style facilitating user portability.

Operational Net Assessment (ONA). A continuously updated operational support process that provides a commander visibility of effects-to-task linkages based on a "system-of-systems" analysis of a potential adversary's political, military, economic, social, infrastructure, and information (PMESII) war-making capabilities. The ONA process identifies key links and nodes within the adversary's systems and facilitates development of options and evaluation of the full spectrum of methods available to influence, neutralize or destroy them to achieve a desired effect or outcome. ONA informs decision-makers from strategic to tactical levels regarding the complementary effects and supporting missions and tasks that can be considered when applying the full range of diplomatic, information, military and economic (DIME) actions to achieve specific effects on an adversary's will and capability in support of national objectives. ONA is a critical enabler for achieving rapid, decisive operations. It is an integrated, collaborative product of Department of Defense and other appropriate government and non-government organization information and data.

Operational Position. As applied to DJC2, an operational position includes a workstation and all required support equipment within the DJC2 system.

Operational Requirements Document (ORD). A formatted statement containing performance based and related operational parameters for the proposed concept or system. Prepared by the user or user's representative at each milestone beginning with Milestone I. Publication CJCSI 3170.01C, has replaced ORDs with CDDs. However, new ORDs were accepted for 90 days after release of the document. Existing ORDs continue to be used until absorbed into the new JCIDS.

Operational View (OV). The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DOD missions. DOD missions include both warfighting missions and business processes. The OV contains graphical and textual products comprising an identification of the operational nodes and elements, assigned tasks and activities, and information flows required between nodes. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges.

Originator. A DOD component or operational command initiating an ICD/MNS. The originator may or may not be the sponsor.

Procedural interface. The methods and procedures employed to establish an interconnection within and between systems or equipment and to transfer information within or between systems or equipment.

Real Time.

a. Pertaining to the timeliness of data or information delayed only by the time required for electronic communication. This implies there are no noticeable delays. (JP 1-02)

b. Timeliness of data or information delayed only by the time required for electronic communication. This implies there are no noticeable delays. Data is real time when current active tracks show current location, updates occur immediately, and the only delay is of electronic communication. (CJCSI 3151.01)

Requirement. The need of an operational user initially expressed in broad operational capability terms in the format of a MNS. It progressively evolves to system-specific performance requirements in the CDD.

Seamless IT and NSS environment. An electronic environment allowing data to be accessed by the warfighter without regard to physical or electronic boundaries.

Server Based Architecture vs. Interactive Web Based Architecture. The analysis examined how the warfighter accesses centers of excellence databases in real-time with a server-based architecture vs. an interactive web-based architecture.

Service Component Command. A command consisting of the Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under that command, including the support forces that have been assigned to a combatant command or further assigned to a subordinate unified command or joint task force. (JCS Pub 1-02)

Service deployment plans and fielding plans. A set of plans describing the evolution from current capabilities to the full operational capability for new or modified IT and NSS. Included are fielding schedules, plans, locations, and associated time-phased interoperability capabilities and requirements with current and planned systems of other DOD components or allies.

Sharable Content Object Reference Model (SCORM). Defines a Web-based learning “Content Aggregation Model” and “Run-time Environment” for learning objects. At its simplest, the model references a set of interrelated technical specifications and guidelines designed to meet the DOD’s high-level requirements for e-learning content.

Shared Spaces.

- Public Spaces: information and resources that are shared with all GIG users

- **Domain Shared Spaces:** partially constrained to highly constrained information and resources that are shared with explicitly identified GIG users. COIs constrain this shared space to varying degrees. COIs can be:
 - Institutional Functional – explicitly recognized, longer term, formalized process based on span of control, relatively few entities [e.g., Principal Staff Assistants (PSAs) such as Logistics]
 - Institutional Cross-Functional – explicitly or implicitly recognized, longer term but priority driven, blended processes resulting in agreements (e.g., Precision Engagement)
 - Expedient Functional – tactically driven, implied authority, formal processes modified for need, relatively many entities (e.g., New Imagery Analysis capability for Damage Assessment)
 - Expedient Cross-Functional – tactically driven, derived authority, ad hoc processes, many entities (e.g., forward deployed JTF planning new threat response)

- **Private Spaces:** non-shared, individual private information and resources

Shared space is a mechanism that provides storage of and access to data for users within a bounded network space. Enterprise-shared space refers to a store of data that is accessible by all users within or across security domains on the GIG. A shared space provides virtual or physical access to any number of data assets (e.g., catalogs, web sites, registries, document storage, and databases). As described in this Strategy, any user, system, or application that posts data uses shared space. (DOD Data Strategy, 9 May 2003)

Single Architecture. A Single Architecture consists of the three views (Operational View, Systems View, and Technical Standards View) of the DOD Architecture Framework (DODAF). The views display different areas of emphasis into an integrated architecture, including defined work processes and supporting Information Technology (IT). The logical linkages among the architecture data elements underlying the products and views ensure the architecture remains mutually consistent. The linkages provide traceability from view to view, from product to product within a view, and across views, ensuring:

- Integration of systems within a Family of Systems (FoS) or System of Systems (SoS),
- Alignment of IT functionality to mission and operational needs, and
- Relationships between current and future systems to current and future standards.

Situational Awareness. Fused battlespace awareness tailored to provide current and projected disposition of hostile, neutral, and friendly forces through near real time/real time sensor data and Service/National/inter-Agency/joint-provided data sources.

Spectrum Certification. The process by which development or procurement of communication-electronics systems, including all systems employing satellite techniques, is reviewed and certified for system compliance with Spectrum Supportability policy, allocations,

regulations, and technical standards to ensure radio frequency spectrum availability. Also, the predicted degree of electromagnetic compatibility between the proposed system and other spectrum-dependent systems and the possible need for and evaluation of the results of prototype electromagnetic compatibility testing is determined.

Spectrum Supportability. The determination of whether the electromagnetic spectrum necessary to support the operation of spectrum-dependent equipment or system during its expected lifecycle is, or is not, available (that is, from system development, through developmental and operational testing, to actual operation in the electromagnetic environment). The assessment of equipment or system as having “spectrum supportability is based upon, as a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation, and consideration of electromagnetic compatibility (EMC).”

Sponsor. The DOD component responsible for all common documentation, periodic reporting and funding actions required to support the capabilities development and acquisition process for a specific capability proposal.

Standardization approach. Statement(s), which demonstrate a commitment to use DOD-approved standards. For example, “The system must comply with applicable information technology standards contained in the DOD Information Technology Standards Registry (DISR) current version.”

Standards. Standards, as referenced in this instruction, are information technology (IT) standards and include specifications, profiles, protocols, implementation conventions, Federal Information Processing Standards (FIPs), Military Standards (MIL-STDs), Defense Performance Specifications (MIL-PRFs), NATO Standardization Agreements (STANAGs), Allied Communications Publications (ACPs), Allied Data Publications (ADatP), guidelines, commercial item descriptions, standardized drawings, handbooks, manuals, tools, and other related documents relevant to the application and use of information and communications technology. They are software and hardware standards used for intelligence collection, data and information processing, information transfer, and information presentation/ dissemination. IT standards provide technical definitions for information system processes, procedures, practices, operations, services, interfaces, connectivity, interoperability, information formats, information content, interchange, and transmission of transfer. IT standards apply during the development, testing, fielding, enhancement, and life cycle maintenance of DOD information systems. Recognized standards include those produced as non-governmental national or international standards (e.g., ANSI and ISO), trade association and professional society standards (e.g., IEEE), Federal standards (e.g., FIPS), military standards, and multinational treaty organization standardization agreements.

Substantive comment. Substantive comments are provided because sections in the document appear to be or are potentially unnecessary, incorrect, incomplete, misleading, confusing, or inconsistent with other sections.

Supportability. The level programs, regardless of ACAT, adequately address IT and NSS infrastructure requirements, the availability of bandwidth and spectrum support, funding, personnel, and dependencies and interface requirements between systems.

System. In this publication, “system” refers to a system or program. A practical definition is a “system” follows the complete Joint Capability Integration and Development System (JCIDS) Requirements Generation System (RGS) process.

System of Systems (SoS). A set arrangement of interdependent systems related or connected to provide a given capability. The loss of any part of the system degrades the performance or capabilities of the whole. An example of a SoS could be interdependent information systems. While individual systems within the SoS may be developed to satisfy the peculiar needs of a given user group (like a specific Service or Agency), the information they share is so important, the loss of a single system may deprive other systems of the data needed to achieve even minimal capabilities. (Defense Acquisition Guidebook V1.0, 17 Oct 2004)

System Training. Includes all training methodologies (Embedded, institutional, Mobile Training Team, computer and web based) which can be used to train and educate operator and maintainer personnel in the proper technical employment and repair of the equipment and components of a system, and to educate and train the commanders and staffs in the doctrinal tactics, techniques and procedures for employing the system in operations and missions. (JT FCB presentation to JCB, “Implementation Brief for System Training as Selective Key Performance Parameter, 2 February 2007)

Systems View (SV). The SV is a set of graphic and text products describing systems and interconnections providing for, or supporting, DOD functions. DOD functions include both warfighting and business functions. The SV associates systems resources to the OV. These systems resources support operational activities and facilitate the exchange of information among operational nodes.

Technical Standards View (TV). The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. It ensures a system satisfies a specified set of operational requirements. The TV provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The TV includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria organized into profile(s) to govern systems and system elements for a given architecture.

Thick Client. A thick client is where the bulk of the data processing occurs on the terminal. In a thick client environment, larger applications are required on the terminals necessitating more robust terminals.

Threshold. A minimum acceptable operational value below which, system utility becomes questionable.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Thin Client. Integral to a net-centric environment, thin client is a low-cost computing device used to access Service/Agency/joint-provided applications and data sources via the GIG/NCES infrastructure. A thin client is where the bulk of data processing occurs on the server. A thin client environment reduces the number of licenses needed to operate applications and enables less capable terminals to operate quickly.

Total Force Visibility. The ability to achieve a current, unobstructed, worldwide view of force/capability inventory and force/capability commitment, availability and readiness; and the ability to readily discern changes in that status. (Global Force Management Document, 4 May 2005)

Unit. 1. Any military element whose structure is prescribed by competent authority, such as a table of organization and equipment; specifically, part of an organization. 2. An organization title of a subdivision of a group in a task force. 3. A standard or basic quantity into which an item of supply is divided, issued, or used. In this meaning, also called unit of issue. 4. With regard to Reserve Components of the Armed Forces, denotes a Selected Reserve unit organized, equipped, and trained for mobilization to serve on active duty as a unit or to augment or be augmented by another unit. Headquarters and support functions without wartime missions are not considered units. (JCS Pub 1-02)

User. Individual or process authorized to access an information system. PKI user: Individual defined, registered, and bound to a public key structure by a certification authority (CA)

Validation. 1. A process normally associated with the collection of intelligence that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not been previously satisfied. 2. In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. 3. Execution procedure used by combatant command components, supporting combatant commanders, and providing organizations to confirm to the supported commander and US Transportation Command that all the information records in a time-phased force and deployment data not only are error free for automation purposes, but also accurately reflect the current status, attributes, and availability of units and requirements. Unit readiness, movement dates, passengers, and cargo details should be confirmed with the unit before validation occurs. (JCS Pub 1-02)

Validation Authority. The individual within the DOD components charged with overall capability definition and validation. The Vice Chairman of the Joint Chiefs of Staff, in the role as Chairman of the JROC, is the validation authority for all potential major defense acquisition programs. The validation authority for JCIDS issues is dependent upon the JPD of the program or initiative as specified below:

- a. JROC Interest - JROC is validation authority.
- b. Joint Impact - The lead FCB is the validation authority.
- c. Joint Integration - The sponsor is the validation authority.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

d. Independent - The sponsor is the validation authority.

X, Y, Z Coordinates. Horizontal (X/Y) and vertical (Z) positioning data, expressed in degrees of latitude and longitude, or meters Northing and Easting, and elevation. Referenced to a local reference datum and vertical datum, or to the World Geodetic System (WGS) and Height Above Ellipsoid (HAE). When using latitude and longitude values, point position may be conveyed in the following formats: Degrees/Minutes/Seconds, and Degrees, Minutes, and Decimals Minute. All reporting of point positioning data must include values of circular and linear error, including confidence intervals.