Charter

for the

Joint Information Environment

Management Construct

Approved by:

Teresa M. Takai
DoD, Chief Information Officer

DATE: NOV -9 2012

REFERENCES

a. DoD IT Enterprise Strategy & Roadmap (ITESR) (5 Oct 11)

b. Joint Chiefs of Staff (JCS) Direction to Establish a Department of Defense (DoD) Information Technology (IT) Effectivenss Department Plan (16 Dec 11)

c. JCS Operational Deputies (OPSDEPS) Update Briefing & Concurrence on the DoD IT Effectivenss End State Architecture (3 Feb 12)

d. JCS Briefing & Approval of the DoD IT Effectivenss End State Architecture (13 Feb 12)

e. DoD 3-Star Programmers Plans Update (1 Mar 12)

f. DoD Deputies Management Advisory Group (DMAG) Plans Update (6 Mar 12)

g. JCS OPSDEPS Update Briefing & Concurrence on the DoD IT Effectivenss Plans of Action and Milestones (POA&Ms) (30 March 12)

h. JCS Briefing & Approval of the DoD IT Effectivenss Plans of Actions and Milestones (17 April 12)

i. DoD DMAG DoD IT Effectiveness Update (6 July 12)

j. JCS OPSDEPS Briefing (9 Jul 12)

k. JCS approved the 13 Jul 12 DoD IT Effectiveness Briefing on the JIE Definition and Characteristics and Transition to Implementation (6 Aug 12)

I. PURPOSE AND SCOPE:

1. This charter is established under the authorities of the Secretary of Defense (SECDEF) decision on 6 October 2010, Department of Defense (DoD) Information Technology (IT) Efficiencies briefing, to move the Department to the Joint Information Environment (JIE). This effort supports the closure of 66 capability gaps identified in the GIG 2.0 Initial Capabilities Document (ICD), dated 29 May 2009 and the GIG 2.0 implementation guidance issued by the Deputy Secretary of Defense (DEPSECDEF), dated 18 August 2011.

2. This document establishes the JIE Management Construct (JMC). The JMC is an organizational and functional framework that establishes activities; defines roles and responsibilities; and specifies processes for implementing, governing, and administering the JIE strategy. JIE processes synchronize the DoD Components Plans of Action and Milestones (POA&Ms) and execution activities while ensuring alignment with the overall Department's IT Effectiveness effort.

3. The JMC is also responsible for identifying compliance issues and making recommendations on resource, requirements and funding shortfalls through the DoD CIO to the Requirements, Budgeting, and Acquisition processes and to the respective DoD Components for resolution. If the DoD Components can resolve the problem, then the JMC will continue to implement the JIE plan. However, when resolution within the DoD Components is not possible, conflicts will be elevated to the appropriate senior governing body (i.e., Deputies Management Group (DMAG), Joint Chiefs of Staff TANK, Joint Requirements Oversight Council (JROC), Defense Acquisition Board (DAB), Chief Information Officers Executive Board (CIO EB), or 3-Star Programmers) for resolution.

4. The JMC will coordinate implementation actions with the potential to impact ongoing operations with transition managers, who coordinate with the Operational Sponsor, theater-level execution sponsor and Joint Technical Synchronization Office (JTSO) to ensure continuity of operations (COOP). For conflicts, the issues will be escalated to the JIE Executive Committee (EXCOM) for resolution.

II. BACKGROUND:

1. The JIE, as approved by the Joint Chiefs of Staff on 6 August 2012, is defined as a secure joint information environment, comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE will be operated and managed per the authorities and responsibilities specified in the Unified Command Plan (UCP) (current and future) using enforceable standards, specifications, and common tactics, techniques and procedures (TTPs).

2. The objective of the JIE is to provide a single, secure, reliable, timely, effective, and agile command, control, communications and computers (C4) enterprise information environment for use by Joint forces and non-DoD mission partners across the full spectrum of operations, at all echelons, and in all operational environments. JIE will support the full range of military operations from military engagement, security cooperation and deterrence activities to defense of the Department of Defense Information Network (GIG 2.0) against kinetic and non-kinetic attacks while at the same time supporting business and intelligence operations of the Department.

3. In addition, JIE supports Homeland Defense and Defense Support of Civil Authorities operations and enables DoD and other interagency mission partners to seamlessly share vital information. JIE also supports humanitarian assistance/disaster relief, peace enforcement, peacekeeping, and show of force operations in addition to supporting multi-national operations, exercises, and training.

4. The governance, operational and technical characteristics listed below were approved by the JCS Operational Deputies (OPSDEPS) as a means of scoping and clarifying the activities of JIE and to provide the boundaries for achieving the objectives of the SECDEF's 6 October 2010 decision on Course of Action 2. The characteristics support the definition of JIE as written above in Section II, paragraph 1. The characteristics are as follows:

a) Network enables mission success in all domains to include agile safe sharing with mission partners.
b) DoD Components retain mission-specific applications when critical for mission success.
c) Allows integration and execution of cyberspace capabilities within, through and across the other warfighting domains.
d) Network is centrally managed, but de-centrally executed.
e) Pre-planned procedures/Cyber Rules of Engagement enable decisions at the lowest level.
f) Common Operational Picture as depicted in the Information Technology Enterprise Strategy and Roadmap.
g) Command and Control (C2) Concept of Operations (CONOPS) describes C/S/As engagement in JIE to enable joint information sharing through a centralized Joint Network Operation and Security organization.
h) Fully optimized set of DoD enterprise-level data & operations centers.
i) Shared situational awareness for all IT activities.
j) Shared IT Infrastructure.
k) Common Enterprise Services, Applications & Tools.

l) Shared services are established to support timely and secure access to protected data and applications.
m) Global Authentication and Directory Services fully interoperable with Intelligence Community (IC) and interagency mission partners.
n) Foundational and shared common services are globally available and accessible at the tactical edge.
o) Access at the point of need.
p) Common Identity Management and Access Control fully interoperable with IC and interagency mission partners.
q) Single Security Architecture.
r) The network and security architecture replaces current C/S/A-specific architectures[1].
s) Data Centric vice Net-Centric.
t) The ability to use velocity, value, variety, and volume of data improves decision making and situational awareness.
u) JIE-approved non-standard interfaces (transport and application layer) allow DoD Components to support mission-unique requirements seamlessly in a joint/combined environment.
v) Reduced number of data centers & servers.
w) Increased percentage of server utilization.
x) Forces in a disconnected, intermittent, low-bandwidth environment maintain the capability to execute mission-critical functions.
y) Initial-entry expeditionary capabilities supported by JIE.
z) Mission assurance (e.g., COOP) is inherent in the design of JIE.

[1] The intent of this characteristic is to highlight the Departments decision to move to a common security architecture that will replace the current Service-centric security architectures as a means to enhance security of the network. It does not imply or preclude any agreements about operations.

III. JIE MANAGEMENT CONSTRUCTS (JMC) Key Functions:

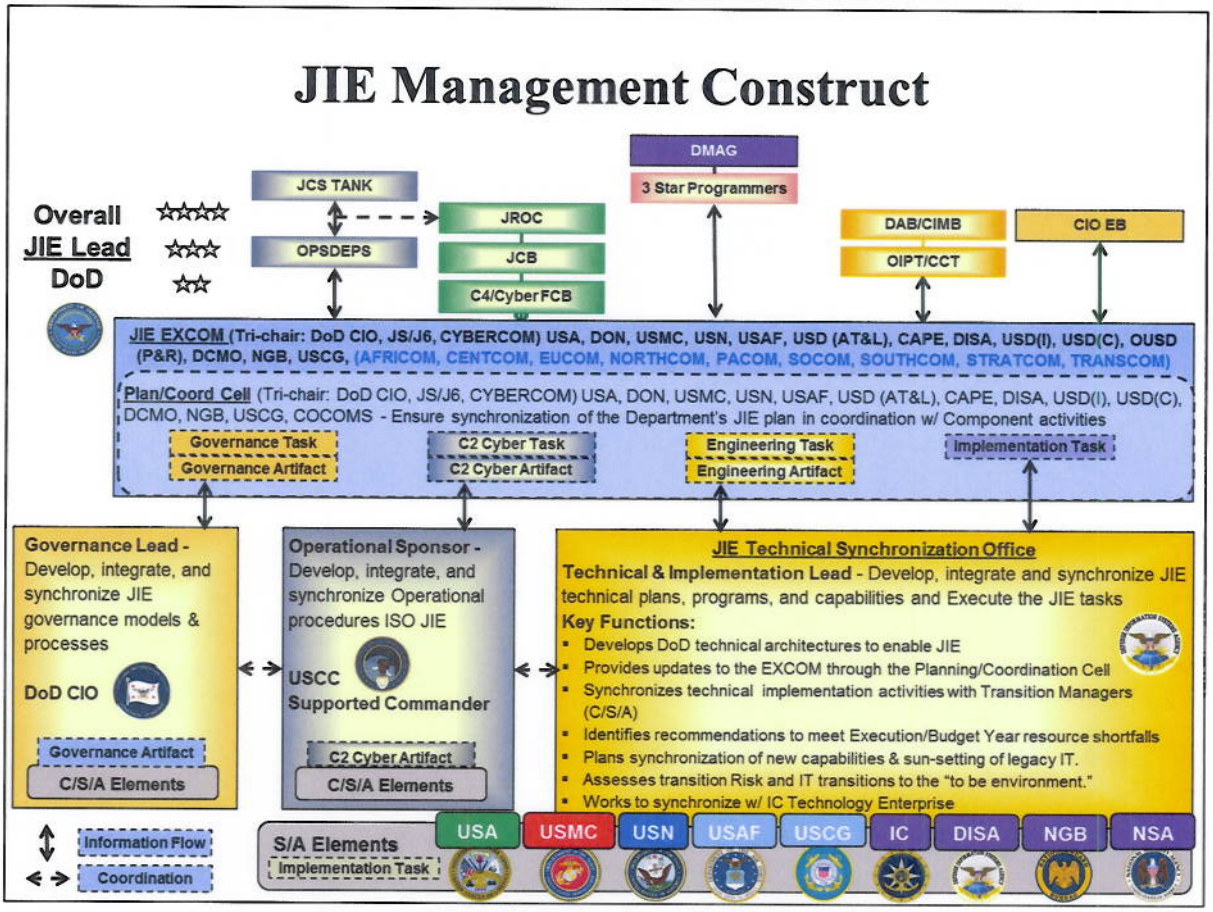

Figure 1. JIE Management Construct

1. The above figure depicts the overall JIE governance structure. At the strategic level, the figure depicts the alignment of JIE with key Department processes. JIE related requirement decisions will be validated by the JROC; Planning, Programming, Budgeting, and Execution (PPBE) decisions will be approved at the 3-Star Programmers or the Deputies Management Action Group (DMAG); and acquisition decisions through Defense Acquisition Board (DAB) and the newly chartered Cyber Investment Management Board (CIMB), if related to Cyber. Additionally, operational decisions are made at the Joint Chiefs of Staff via the TANK. The DoD CIO is charged with making Department-level recommendations on IT related policy, budgetary and acquisition decisions as well as leading the overall JIE initiative. Sections 1 through 7 below highlight the functions of the JIE Executive Committee and the subordinate JMC structure.

2. JIE Executive Committee (EXCOM)[2]:

a) Sets the JIE direction, establishes goals and objectives, and provides oversight and maintains accountability.
b) Develops JIE plans, policies and governance approaches; initiates review of issues, IT related programs, initiatives and systems considered essential for enterprise-wide solutions and operational effectiveness; provides JIE standards; recommends investments and enforces compliance.
c) Provides decisions on the JIE execution plan. Elevates operational issues through the DoD Chief Information Officer (CIO) to OPDEPS in coordination with United States Cyber Command (USCYBERCOM). Elevates resourcing issues through the DoD CIO to the 3-Star Programmers and Deputies Management Action Group (DMAG) for decision. Elevates acquisition issues to the USD(AT&L) for review and /or decisions.
d) Authorizes additional permanent and temporary working groups, as necessary, to facilitate execution of JIE tasks.

3. JIE Planning and Coordination Cell: Ensures the synchronization of DoD Components actions to realize an integrated Department-wide implementation of the JIE.

a) Coordinates Component and leadership updates.
b) Maintains the Integrated Master Schedule, tracks Implementation Plan and maintains overall JIE CONOPS.
c) Synchronizes Plan of Actions and Milestone (POA&M) compliance with the Components' activities.
d) Ensures the coordination and synchronization of activities of the Governance, Operational, and Technical elements.
e) Coordinates resource planning, execution and Unfunded Requirements tracking.
f) Manages implementation issue resolution and execution on behalf of the JIE EXCOM as depicted in Section I, paragraph 3. above.
g) Develops and publishes standardized JIE Strategic Communications.

4. Governance (DoD CIO): Develops, integrates, and synchronizes governance.

a) Provides the overarching plans, guidance and policy that inform requirements approval, Enterprise Architectures development and Department IT processes.
b) Coordinates planning and resourcing activities.

---

[2] The JIE EXCOM is a General Officer/Flag Officer/Senior Executive Service (GO/FO/SES) level meeting. Representatives who attend in lieu of the assigned Principal are empowered to speak for their organizations.

c) Reviews JIE Service Level Agreements (SLAs) and/or Memoranda of Agreement (MOAs).
d) Updates the EXCOM through the Planning and Coordination Cell.

5. Operational Sponsor (USCYBERCOM): Develops, integrates and synchronizes operational procedures in support of JIE IAW with Department-level procedures.

a) In coordination with the theater-level execution sponsor(s), coordinates and leads the development of:
   1) JIE C2 Cyber Construct/Implementation.
   2) Tactics, Techniques and Procedures (TTPs) and Standard Operating Procedures (SOPs).
   3) Operations (OPS) Center accreditation process.
   4) Concept of Operations (CONOPS).
   5) Configuration of Enterprise Management Services (EMS) tools.
   6) TTPs necessary to operate and maintain Authoritative Data Repository for operational related artifacts.
b) Monitors and reports on operations.
c) Assesses operational risk.
d) Monitors SLA performance and tracks metrics.
e) Enforces operational compliance.
f) Synchronize Continuity of Operations (COOP) and Disaster Recovery (DR) plans.
g) Identifies and makes recommendations on budgetary priorities, necessary for JIE operations, through the JMC in coordination with Combatant Command Integrated Priority Lists and Cyber Component inputs.
h) Updates the EXCOM through the Planning and Coordination Cell.

6. JIE Technical Synchronization Office (JTSO) (DISA): Serves as the Technical and Implementation Lead and provides engineering and architectures. Develops, integrates and synchronizes JIE technical plans, programs, and capabilities to realize an integrated Department-wide implementation of the JIE. The JTSO:

a) Leads the development of DoD technical specifications to enable JIE.
b) Updates the EXCOM through the Planning and Coordination Cell.
c) Serves as Technical Configuration Manager.
d) Manages the overall Department's Plan of Action and Milestones (POA&M).
e) Makes recommendations to meet Execution/Budget Year resource shortfalls.
f) Plans synchronization of new capabilities & sun-setting of legacy IT.

g) Conducts Transition Risk assessments and synchronizes IT transitions to the "to be" environment.
h) Ensures key enterprise services are aligned and interoperable to allow information sharing with the IC Information Technology Enterprise.
i) Leads development of Technical Designs and Specifications.
j) Provides input into Capability Requirements Documents (CRD).
k) Develops Implementation plan(s) and synchronizes implementation activities with Transition Managers (DoD Components).
l) Leads technical surveys, assessments, and reviews.
m) Assesses technology innovation and insertion process.
n) Leads development of Data Repository structures to enable storage of JIE related artifacts.
o) Provides Technical input to Business Case Analyses (BCAs) and Analysis of Alternatives (AOAs).
p) Provides Enterprise contracting capabilities.
q) Maintains service catalogues.
r) Manages JIE-related SLAs and MOAs.
s) Coordinates activities with governance and operational activities as appropriate.
t) Ensures security architecture development is designed to secure the infrastructure, provide access and allow data sharing across the environment.

7. Combatant Commands: Serve as the theater-level execution sponsor for incremental delivery of JIE capabilities.

a) Establish a theater-level governance structure to synchronize and integrate theater-level actions necessary to deliver JIE.
b) Identifies issues, risks, and obstacles to the JIE EXCOM through the Planning and Coordination Cell.
c) Synchronizes Component's POA&M(s) in support of theater-level execution.
d) Participates in required JIE-related working groups.
e) Ensures synchronization of JIE implementation with OPLANS and CONPLANs.
f) Oversees development of specific COOP and DR plans

8. Implementers (DoD Components): Engineer, implement, and operate the JIE for their respective organizations to move the Department closer to the delivery of JIE capabilities. They also identify obstacles and issues that may impede delivery of JIE capabilities and recommend solutions. Each organization will appoint a Transition Manager, who manages implementation and ensures continuity of operations as organizations transition from the "as is" to the "to be" in coordination with the theater-level execution sponsor.

a) Identifies issues, risks, and obstacles to the JIE EXCOM through the Planning and Coordination Cell.
b) Develops the Component's POA&M and provides input to the overall Department's POA&M.
c) Participates in required JIE working groups.
d) Provides JIE status updates.
e) Manages JIE resources for funding execution.
f) Provides input to implementation plans.
g) Develops the specifics plans and ensures execution of COOP and DR plans

IV. MEMBERS ROLES AND RESPONSIBILITIES: (Voting and non-voting designations apply at all level of the JIE Governance process.)

1. DoD CIO: Provides overall governance and direction for JIE Implementation. Tri-chairs the JIE Executive Committee and the JIE Planning and Coordination Cell. Voting member.

2. Undersecretary of Defense Acquisition, Technology, and Logistics (AT&L): Exercises Milestone Decision Authority for JIE, unless delegated, and subsequently approves the appointment of a Component Acquisition Executive. Voting member.

3. Undersecretary of Defense (Comptroller) and Chief Financial Officer (CFO): Provides the overall Financial Management Framework and guidance for resourcing the JIE through the Department's PPBE processes, to include overseeing the financial policy and the use of the financial management systems. Voting member.

4. Undersecretary of Defense (Intelligence): Synchronizes Intelligence Community efforts with JIE architecture and Service solution architectures to ensure global operations are adequately planned and exercised. Serves as the DoD Intelligence Mission Area advisor to JIE. Voting member.

5. Undersecretary of Defense for Personnel and Readiness (OUSD P&R): Serves as the Total Force Management advisor as it relates to readiness; National Guard and Reserve Component Affairs; health affairs; training; personnel requirements and management to include equal opportunity. Morale, welfare, recreation, and quality of life matters to the JIE. Synchronizes total force management automation capabilities, operations and governance with JIE. Voting member.

6. Deputy Chief Management Officer (DCMO). Serves as the Business Mission Area (BMA) advisor to the JIE. Synchronizes business automation operations with JIE. Voting member.

7. Cost Assessment and Program Evaluation (CAPE): Provides the overall Department-level analytical framework for evaluation of plans, programs and budgets through the Department's PPBE processes. Voting member.

8. Joint Staff (JS): Validates JIE requirements and tri-chairs the JIE Executive Committee and the JIE Planning and Coordination Cell. Serves as the Warfighter Mission Area advisor to JIE. Voting member.

9. United States CYBER Command (USCYBERCOM): Serves as the Operational Sponsor and tri-chairs the JIE Executive Committee and the JIE Planning and Coordination Cell. Voting member.

10. National Security Agency (NSA). Serves as the Security Advisor for JIE and will be recognized as part of the JTSO. Non-voting member.

11. Defense Information Systems Agency (DISA): Leads the JIE Technical Synchronization Office and serves as the Technical and Implementation Lead. Voting member.

12. DoD Components: Implements the tasks necessary to execute the JIE plan and serves as the Transition Managers. Voting members: DON, USA, USN, USAF, USMC, USCG and NGB.

13. Combatant Commands (COCOMs): Responsible for setting the priority of activities and ensuring alignment of the Departments approved strategic plan of action and milestones with operations to produce a theater level implementation schedule and plan. Voting member through the JS J6.[3]

V. TIMELINE: Effective on date of signature. Duration is until a formalized Department IT governance structure is established.

VI. RESOURCING: This charter does not constitute an agreement to transfer funds or Full Time Equivalents (FTEs).

[3] The JIE EXCOM will ensure that the PCC, Governance, Operations, and JTSO have established processes on behalf of the COCOMs to enable participation and review for technical, operational, and governance decisions and conflict resolution. The Joint Staff will ensure all COCOM equities are considered, represented, and factored into all JIE decisions.

ACRONYMS

AFRICOM	Africa Command
AOAs	Analysis of Alternatives
BCAs	Business Case Analyses
C/S/As	Combatant Commands/Services/Agencies
C2	Command and Control
C4	Command, Control, Communications and Computers
CAPE	Cost Assessment and Program Evaluation
CCT	Cyber Capabilities Team
CENTCOM	Central Command
CIMB	CYBER Investment Management Board
CONOPS	Concept of Operations
CONPLANs	operation plans in concept format
COOP	Continuity of Operations
CRD	Capability Requirements Documents
DAB	Defense Acquisition Board
DCMO	Deputy Chief Management Officer
DISA	Defense Information Systems Agency
DMAG	Defense Management Advisory Group
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DR	Disaster Recovery
EMS	Enterprise Management Services
EUCOM	European Command
EXCOM	Executive Committee
FCB	Functional Capability Board
FTEs	Full Time Equivalents
GIG	Global Information Grid
IC	Intelligence Community
ICD	Initial Capabilities Document
ISO	in support of
IT	Information Technology
JCB	Joint Capability Board
JCS	Joint Chiefs of Staff
JIE	Joint Information Environment
JMC	JIE Management Construct
JROC	Joint Requirements Oversight Council
JS	Joint Staff

ACRONYMS (continued)

JS/J6	Joint Staff Command, Control, Communications, & Computers/Cyber
JTSO	JIE Technical Synchronization Office
MOAs	Memoranda of Agreement
NGB	National Guard Bureau
NORTHCOM	Northern Command
NSA	National Security Agency
OIPT	Overarching Integrated Product Teams
OPLANS	operation plans
OPS	Operations
OPSDEPS	Operations Deputies
PACOM	Pacific Command
Plan/Coord Cell	Planning and Coordination Cell
POA&Ms	Plans of Action and Milestones
ROE	Rules of Engagement
SECDEF	Secretary of Defense
SLAs	Service Level Agreements
SOCOM	Special Operations Command
SOPs	Standard Operating Procedures
SOUTHCOM	Southern Command
STRATCOM	Strategic Command
TRANSCOM	Transportation Command
TTPs	Tactics, Techniques, and Procedures
UCP	Unified Command Plan
USA	United States Army
USAF	United States Air Force
USCG	United States Coast Guard
USCYBERCOM	United States CYBER Command
USD(I)	Undersecretary of Defense (Intelligence)
USD/AT&L	Undersecretary of Defense Acquisition, Technology, and Logistics
USD(C)	Undersecretary of Defense (Comptroller) and Chief Financial Officer (CFO)
USMC	United States Marine Corps
USN	United States Navy