DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

SEP 26 2013

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Joint Information Environment Implementation Guidance

References: (a) Deputy Secretary of Defense Memorandum, Strategic Choices and Management Review Resulting Direction and Guidance, July 1, 2013
(b) Deputy Secretary of Defense Memorandum, Joint Information Environment Implementation, May 6, 2013
(c) Department of Defense Chief Information Officer Charter, Joint Information Environment Management Construct, November 9, 2012
(d) Secretary of Defense Execution Order, Joint Information Environment, December 5, 2012

In accordance with (IAW) references (a) and (b) above, this memorandum outlines how the Department of Defense Chief Information Officer (DoD CIO) will oversee and manage Department-wide activities to implement Joint Information Environment (JIE). Sustained partnership and continued participation from DoD Components remains critical to define and implement the decisions of JIE governance and Integrated Master Schedule. These decisions prioritize and direct actions utilizing the Department's requirements, budgeting, investment, and acquisition processes in order to realize the JIE vision. The following provides the details necessary to facilitate delivery of JIE.

The attached Guidance for Implementing the JIE outlines our approach to the objective enterprise end-state. Our first steps include the design and implementation of common Information Technology (IT) capabilities comprising Network Normalization, Core Data Centers, Enterprise Services, and Identity and Access Management (IdAM) established on a

single security architecture foundation for JIE. Enterprise Operations Centers and Help Desk construct will be implemented to manage and operate this environment.

The implementation of JIE requires unprecedented dedicated support and cooperation to achieve this major Department objective. Within 120 days of the date of this memo, the Military Services and Defense Information Systems Agency (DISA) should submit their plans for how they will support the actions outlined in Figure 2 of the attached JIE Implementation Guidance. Where the dates are determined to be unachievable, alternative dates should be proposed. Guidance on reporting of JIE Implementation status will be provided in a separate memo. These reports will support periodic updates to DoD Senior Leadership on the Department's progress to achieve the JIE end state.

Strong governance is required to effect change on this scale. As overall lead, I will use the JIE Executive Committee (EXCOM) IAW reference (c) with subgroup responsibilities listed below:

- The JIE Management Office (JMO), which includes the DoD CIO members of the JIE Planning and Coordination Cell (PCC), will work across the DoD CIO organization, Military Departments, 4th Estate, and DISA to achieve the envisioned JIE.

- The JIE PCC will maintain the Integrated Master Schedule, execute JIE EXCOM decisions, and enable synchronization of Component activities with the JIE governance, operations, and technical implementation.

- The JIE Governance working group will evolve the Department's overall IT governance by framing an enduring structure that strengthens Command, Control, Communications and Computers (C4) Cyber/IT management and governance.

- The Joint Operations Sponsor Group will develop the common Tactics, Techniques, and Procedures/Standard Operating Procedures necessary to operate and defend the JIE.

- The JIE Technical Synchronization Office will lead the engineering and development of the enterprise capabilities solutions designs.

If Components do not have representation on these JIE activities, please submit your representative's contact information to the e-mail address listed below.

I will stand up an IT Investment Review Board to develop a DoD-wide IT investment strategy and monitor execution of the Department's IT budget to facilitate delivery of the capabilities contained within the JIE Plan of Actions and Milestones. Additional milestones to

complete Increment 1 will be captured in the JIE Integrated Master Schedule in support of DoD CIO Capabilities Planning Guidance.

IAW reference (d), I will continue to work with the Director, Joint Staff and the Commander, US Cyber Command to provide JIE transformation planning and execution guidance for DoD Components. As JIE implementation evolves, follow-on modifications to the JIE EXORD with specific tasks and responsibilities will be issued.

Finally, I applaud the Combatant Commands', Services', and Agencies' ongoing initiatives that will provide key enabling infrastructure and services to the JIE. While the Department continues to formalize JIE, our focus will be to identify and synchronize the daily actions that are happening to enable the effort. Your sustained involvement is essential to this endeavor. Questions regarding JIE may be directed to the JMO at (571) 372-4906, or email at: osd.pentagon.dod-cio.mbx.dcio-ie-workflow@mail.mil.

Teresa M. Takai

Attachment:
As stated

Guidance for Implementing the Joint Information Environment

September 12, 2013

Guidance for
Implementing the
Joint Information Environment (JIE)

Table of Contents

A. Overview

This Guidance for Implementing the JIE provides additional details as directed by the Deputy Secretary of Defense's (DSD) JIE Implementation Memo of May 6, 2013. It also amplifies the DSD's "Fiscal Year (FY) 2015-2019 Fiscal Guidance" to the DoD CIO, which is contained in his "Strategic Choices and Management Review Resulting Direction and Guidance" memorandum of July 1, 2013. Specifically, the July 1, 2013 memo directs the Department to "migrate to the Joint Information Environment (JIE) as rapidly as possible." The Joint Information Environment (JIE) is an effort to fundamentally realign and restructure how the Department's Information Technology (IT) networks, systems, and services are constructed, operated, and defended.

The JIE framework is ambitious and its implementation aggressive. However, DoD has a plan that, when successfully executed, will result in a JIE that will be a force multiplier for improving mission effectiveness, enhancing cyber security, and reducing costs. Implementing this framework is the next step in transforming the DoD's IT infrastructure and the cyber warfighting domain.

I*ncreasingly, DoD mission success depends* upon the ability of military commanders and civilian leaders to act quickly and effectively, *based on the most accurate and timely data and information available*. *JIE is a framework for DoD IT modernization.* It consists of overarching architectures, standards, and specifications; common ways of operating and defending; and common-engineered solution designs implemented across the Department. Anticipated benefits to the DoD from the JIE include:

- Enhanced data access and information sharing
- Improved mission effectiveness
- More effective training
- Increased security
- Optimized resources and IT efficiencies

This guidance describes the main elements of the JIE, highlights their value, and requests DoD Components' support to help accelerate the effort and thereby rapidly deploy the foundational capabilities needed to attain these benefits.

A (1) Characteristics of the JIE

Introduction

The Department intends to provide a secure, reliable, and agile command, control, communications, and computing (C4) enterprise information environment for use by the Joint forces and non-DoD mission partners across the full spectrum of operations. In this context, DoD users worldwide are part of the JIE.

For these end users, the JIE will be akin to a utility – *always available when and where it is needed*. This dynamic combination of technologies, people, and services for DoD users will include:

- Set of applications across DoD for like services
- Standardized architecture, and a robust and resilient infrastructure

- Common operational tactics, techniques, and procedures (TTP's)
- Agile enterprise help desk user support
- Highly trained workforce
- Standardized roles and responsibilities at each operational level

DoD's first steps focus on the creation of a shared IT infrastructure to be used across the Department based on enterprise standards, specifications, and configurations. For those DoD Components that operate and maintain portions of the shared IT infrastructure, they will do so in accordance with enterprise technical and operational standards. *This shared IT infrastructure will look, feel, and operate the same way regardless of service provider and/or use* (such as mission-specific utilization), through adherence to common enterprise-wide TTPs that will improve security.

To outline the JIE implementation plan vision and roadmap, the description below *outlines technical and operational characteristics of the JIE*, with a particular focus on the following technical characteristics:

- Single Security Architecture
- Normalized Federated Networks
- Identity and Access Management (IdAM)
- Data Center Consolidation
- Software Application Rationalization and Server Virtualization
- Desktop Virtualization and Thin-Client Environments
- Mobility Services
- Enterprise Services
- Cloud Computing

Technical Characteristics of the JIE

Technical characteristics of the JIE's shared IT infrastructure include a network that is defendable and virtually single – from tactical to strategic; Department-level consolidation of data centers and network operations centers; and a common security architecture. Those capabilities required across DoD to enable *information sharing, collaboration, and interoperability* will be provided as Enterprise Services that can be provided in federated, franchised, or centralized business models. Any DoD Component may become a service provider for one or more designated Enterprise Service or infrastructure offerings, and when they do so, then the organization will be able to provide those services to the entire Department.

Key technical characteristics of the JIE include those described below.

Single Security Architecture (SSA) will address unique DoD operational mission user requirements while protecting DoD's IT infrastructure through a common Department-wide network security architecture. Benefits of SSA are intended to be reduction of the complexity and cost of network defense; improvement of DoD's security posture and support for mobile, embedded, and other users; decreased operational duplications; improved network resiliency; the establishment of joint protections

and responsibilities across Communities of Interest (COIs); and flattening of the complexity and cost of network defense. In addition, SSA will enable DoD to support COIs on the network across multiple regions and increase effectiveness by improving interoperability and information sharing. Finally, SSA will increase the Department's network security by separating server computing and traffic from end-user devices; implementing physical and logical separations of computing zones in accordance with the JIE Single Security Architecture; move all public facing DoD Servers to Demilitarized Zones (DMZs) to reduce the potential spread of cyber-attack; dividing the network into manageable and securable zones that enforce consistent policies; placing sensors at the most efficient locations for traffic capture and inspection; improving data protections; and supporting the centralization and consolidation of the operations centers, tools, and personnel that operate and defend the network.

Establishing and enforcing an SSA will collapse network security boundaries; reduce the Department's external attack surface; and standardize management, operational and technical security controls. Benefits will include ensuring the confidentiality, integrity, and availability of the DoD's information assets within all required mission contexts, while facilitating rapid attack detection, diagnosis, containment, and response. To establish an SSA, the Department is leveraging the technical and operational expertise of the National Security Agency (NSA) and the participation and support of DoD Components in designing, certifying, accrediting, and testing standardized security suites that will be located at optimal locations. Implementing these standardized security suites at the selected locations will also allow DoD Components to remove existing redundant security suites, which will free resources to be repurposed and applied to fill other gaps. *The JIE SSA will provide DoD cyber forces with decision support capabilities to observe, diagnose, act, maneuver, and dependable mission execution in the face of cyber warfare by a capable cyber adversary.*

Normalized Federated Networks: DoD's current system of disparate network, processing, and storage infrastructures presents more opportunities for improvement. This sometimes incompatible mixed environment impedes internal and external collaboration and places the warfighter and their support elements at the seams of integration. Accordingly, a critical foundational aspect of the JIE vision is to provide a single, secure, information environment that interconnects warfighters securely, reliably, and seamlessly at a reduced cost. By federating networks that employ common operational standards, the Department will enable the sharing of resources among multiple independent networks, such as IT infrastructure, enterprise services, unified communications, and cloud computing services and thereby support the use of mobile devices and thin-client end-user technologies.

DoD will continue normalizing and consolidating its network infrastructure at the Base/Post/Camp/Station or equivalent levels to enterprise level standards and implementation guidance. Service-level programs that facilitate this normalization and consolidation include the Air Force Network (AFNET) migration. The Navy also has its Consolidated Afloat Network and Enterprise Services (CANES) and Next Generation Enterprise (NGEN) for its afloat and ashore infrastructures, respectively. The Department also will broaden planning and implementation of network technologies, such as Multi-Protocol Label Switching (MPLS), which will enable the Department to protect the backbone routers, enable segmentation of planes to better protect against

and isolate threats, and to contain malicious activity. The JIE will implement separate network planes for operations, defense, data replication and synchronization, and user activity in the JIE environment.

Identity and Access Management (IdAM) is fundamental to the security of data and secure information sharing for the DoD. Identity Management creates and administers "identities" that uniquely and unambiguously distinguish people and machines, on all networks, end-to-end across the enterprise. These capabilities are key to the dual JIE goals of increasing the security of the DoD's IT while also increasing mission effectiveness. IdAM services will allow authorized person and non-person entities to securely access DoD resources, anywhere, at any time.

This new expanded approach will update the current manually intensive, inconsistent, time-consuming and resource-heavy local administrative account provisioning and information system access management capabilities. Instead, new IdAM capabilities will maximize the automation of routine access control over IT systems. This will make system access dynamic, ensure entity discovery, and enable activity monitoring and attribution. These capabilities include completely automating the generation of user accounts based on Non-secure Internet Protocol Router (NIPRNET) common access cards (CACs) and Secret Internet Protocol Router Network (SIPRNET) tokens, and making real time information access control decisions based on requesting user attributes, such as clearance, rank, and job function. Use of DoD Public Key Infrastructure (PKI) credentials will be maximized for every login to the NIPRNET / SIPRNET and for every access to any NIPR/SIPR DoD web site. Use of PKI credentials will also permit more effective monitoring and attribution, which will help those who operate and defend DoD networks better understand who is on the DoD networks and what they are doing while on the network.

JIE will have enterprise white pages directory services to allow DoD users to discover other DoD users for collaboration (e.g., voice, email, and chat). This approach will also allow DoD to move away from today's large active directory structures to a more internet like model in which client software on workstations authenticates directly to servers in the cloud without the need for active directory trust relationships.

Data Center Consolidation is critical to improving DoD-wide efficiencies. The current array of DoD data centers, networks, and systems have resulted in unnecessary costs, limited interoperability, and introduced cyber security risks. To address these areas of concern, DoD is executing consolidation efforts that will ultimately reduce the number of data centers, shrink the size of the attack surface, physically separate public facing DoD web servers from mission servers in accordance with the DoD Demilitarized Zone (DMZ) Security Technical Implementation Guides (STIGs), and improve survivability by consolidating and eliminating all data centers that are not part of the target architecture. Data center consolidation will help improve the DoD's ability to streamline security, locate information, and incorporate new technologies and innovative approaches.

DoD will consolidate computing power by closing and consolidating data centers across the Department as part of the Federal Data Center Consolidation Initiative (FDCCI). An important aspect of this effort is the JIE Core Data Center (CDC) initiative, including identifying existing data centers to be

transitioned into JIE CDCs. CDCs will provide highly available, fast, and secured connections to any application or service from any authorized network at any time. From a hosting perspective, CDCs will be the required solution for the Department's enterprise services, DoD Component-specific IT services and applications, and DoD's cloud service delivery model. Cloud computing technologies enabled within the JIE CDCs, as well as through various commercial service providers, will allow the Department to logically consolidate and share commodity functions, which will result in the more efficient use of resources. These efforts will help accelerate related efforts to normalize, rationalize, and reduce the number of the functional software applications that it has in use, to drive out duplicative and unnecessary applications that increase licensing and support costs.

Software Application Rationalization and Server Virtualization will enable additional IT efficiencies. DoD Components are completely rationalizing, normalizing, standardizing, and, to the extent possible, virtualizing the software applications used by the Department, frequently in conjunction with data center consolidation. Application rationalization facilitates optimization of hardware, software, and support for IT systems and applications. DoD will enforce milestones that drive DoD Components to sunset duplicative applications and functionality. Increased application virtualization will reduce costs for facilities maintenance and operations, as well as for server operations and maintenance, and it will improve automation for server management and provisioning.

Desktop Virtualization and Thin-Client Environments are part of a DoD commitment to adopting more efficient approaches to end-user desktop environments, which are one of the most manpower intensive aspects of DoD IT operations and defense. Virtual desktop environments already are in limited use across the Department; over time, the JIE will further extend, accelerate, and standardize their implementation throughout DoD. In addition, virtual desktops are a critical piece of DoD's mobility strategy. Their widespread use will enable users to access their personal desktop—hosted in a JIE CDC—from any thin client, from any DoD location. Likewise, users also can access their virtualized desktops and applications from DoD-approved tablets, pad computers, or smartphones. Use of virtualization will also significantly improve cybersecurity posture by enabling rapid configuration changes across data center applications and creation of pristine operating environments for DoD users for each login session.

Mobility Services are being pursued by DoD as part of a phased approach to mobility solutions, leading to improved unclassified and classified mobile capabilities, under the auspices of the DoD CIO Executive Board. Pilots are underway to refine Mobile Device Management (MDM) and Mobile Applications Store (MAS) requirements, influence commercial standards, and incorporate mobile users into JIE. MDM enables policy enforcement for end-user devices at application and user levels, malware detection, over-the-air software distribution, remote data wiping and device-management configuration, and protection against key and data compromise. Mobile applications are a critical enabler for service delivery and will provide new opportunities to improve mission effectiveness. DoD is establishing an enterprise MAS capability that operates in conjunction with the MDM system and that can deliver, update, and delete applications on mobile devices without requiring users to return the device for service.

Enterprise Services that range from critical business office functions to enterprise applications supporting cross-functional missions have been identified by the Department as either customer-facing or infrastructure Enterprise Services. These high-value services will provide a basis for the initial standup of the JIE CDCs. Candidates for Enterprise Services that DoD CIO has identified include Defense Enterprise Email, Enterprise File Sharing, Unified Capabilities, Enterprise Cross-Domain information transfer services, and Enterprise File Delivery. The Defense Information Systems Agency (DISA) is currently providing or planning the candidate Enterprise Services identified above to support customer-facing capabilities, machine-to-machine services, and infrastructure services.

While current Enterprise Services are developed to support the DoD's business processes at higher enterprise levels, there are insufficient Enterprise Services to support forward deployed users. Even when enterprise-level services are modified and pushed to the tactical-edge users, they are often incompatible with changing environmental factors. As a result, these services are unavailable to consumers, because they cannot function within disconnected, intermittent, or low-bandwidth (DIL) information environments. The DoD CIO will be placing additional emphasis on developing and deploying Enterprise Services that are designed to operate in deployed DIL in future JIE increments. *Providing a consistent set of enterprise services will help ensure that Joint warfighters and their mission partners can discover, access, and use information assets to achieve mission success, no matter where the information resides*.

DoD will continue to accelerate the implementation of Enterprise E-mail and begin implementing complementary capabilities, such as Enterprise SharePoint and File Storage, which will provide the warfighter with increased capabilities at a lower cost. At the same time, the Department must stress the need to sunset DoD Component legacy systems/services as JIE helps ensure that Enterprise Services become operational.

Cloud Computing: Myriad Department-specific cloud computing challenges require careful adoption considerations, especially in cybersecurity, continuity of operations, and resilience. Particular challenges include:

- Achievement of real-time visibility into all cloud activities, where consumers do not have physical control over their systems
- Implementation of continuous monitoring
- Intrusion detection and alerts, as well as diagnosis and response
- Service acquisition and funding sustainment
- Data migration and management
- Overcoming network challenges of tactical-edge users

Department efforts to address these technical challenges to cloud computing include:

- DoD CIO updates to the Department's cybersecurity policies and instructions, and alignment of cybersecurity controls and processes with those used across the federal government.
- Use of the Federal Risk and Authorization Management Program (FedRAMP) for low

sensitivity data; FedRAMP will establish a standard approach for assessing and authorizing cloud computing services.

- Definition of requirements for the continuous auditing and monitoring of cloud service providers.

Cloud computing capabilities will also benefit the Department through increased effectiveness of missions and security segmentation, as well as enhanced operational efficiencies.

Operational Characteristics of the JIE

The JIE is much more than just a new set of IT technologies. DoD IT operations today are limited by DoD Component-centric, non-standardized, non-integrated, and in some cases, non-interoperable capabilities. One of the core elements of JIE is that DoD network operators and defenders must work as one team. The JIE will enable network and system operators and defenders at every level to have visibility into the status of the networks, as well as enable commonality in how cyber threats are countered by DoD. The Department will know who is operating on its networks and what they are doing, and it will be able to attribute their actions with a high degree of confidence. This will minimize complexity for synchronizing cyber responses, maximize operational efficiencies, and reduce risk. The JIE is introducing new concepts and ways of doing business, but it will still be operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common TTPs.

A (2) Acquisition Approach

The JIE is not an acquisition program. Its primary focus is to consolidate, standardize, and optimize. In order to facilitate implementation of JIE through acquisition across the Department, new IT programs will be required to comply with the JIE. Existing IT programs will be mandated to address JIE requirements as they progress through their lifecycle, and decisions will be made on how they can best comply with the JIE.

The ability to influence and effect outcomes of acquisition programs and IT acquisition of services will be a critical component to successful sustainment of the JIE. Current acquisition governance structures offer numerous means by which acquisition programs can be influenced. *In order to obtain the full range of objectives for the JIE, a variety of approaches will be taken in parallel to affect the changes necessary to implement the JIE.*

Implementing JIE reinforces the continued need for “commodity IT” acquisitions across DoD. These include cloud-based services, such as storage, virtual machines, and web hosting; help desks; and hardware/software acquisition. For example, DoD’s current cloud broker implementation provides a front-end coordination for cloud services, to include addressing security requirements; however, there are opportunities for additional centralized acquisition.

A (3) Governance and Oversight

The DoD CIO, working with the DoD Comptroller, will develop more consistent methods to identify cyber and IT funds within DoD Component Programs of Record (PORs). Program Element (PE) accounting codes should be aligned to support identification and tracking of those expenditures

associated with the JIE. Enabling the Department to take full advantage of its collective purchasing power will require incentivizing and encouraging increased use of enterprise commodity purchases.

Implementing the JIE depends on the success of existing DoD Component initiatives. The current and anticipated fiscal environment mandates that the Department leverage and build upon these and other DoD Component activities. Therefore, it is vital that the activities listed in Section A (1) above, and others like them, continue to be adequately resourced and executed on schedule. Leveraging and building on existing and planned activities also will provide DoD with opportunities to align organizational IT efforts to the JIE vision and enable Department leadership to track and make required corrections.

A (4) JIE Implementation Tasks and Guidance

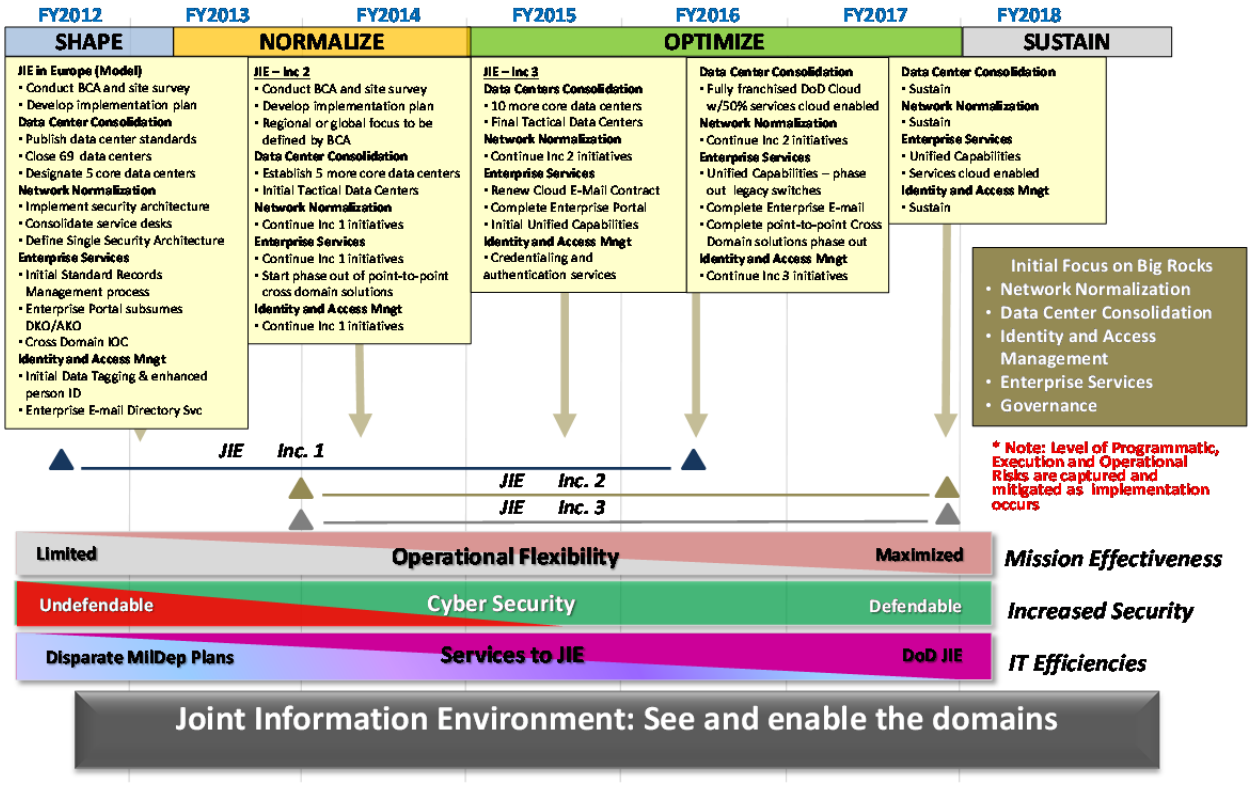
Introduction

Implementation of JIE Increment 1 focuses on the European Area of Responsibility, and it supports the mission areas of United States European Command and United States Africa Command. This approach allows DoD to concurrently deploy enabling infrastructure capabilities and enterprise services that reach beyond a single geographic area. It also will enable the Department to minimize risks and leverage valuable lessons learned as JIE architectural artifacts, processes, and TTPs mature in design and development, and use them in other increments and geographic areas.

The JIE framework will fundamentally change how DoD implements, operates and defends its IT – it is vital to the Department's efforts to increase network security, decrease IT costs, and enhance network resiliency. To most effectively accomplish this significant realignment and restructuring of the Department's IT framework, JIE implementation is taking an incremental and phased approach.

The current JIE approach incorporates three initial incremental implementations layered on top of budgeted IT modernization of its IT infrastructure: Increment 1 focuses on the European Theater; Increment 2 focuses on the Pacific Theater; and Increment 3 will focus on completing actions in CONUS, as well as incorporating emerging capabilities. Planning for the JIE continues to evolve and to date has addressed only Increment 1 in detail. See Figure 1.

Figure 1. JIE Roadmap



Therefore, this section identifies JIE implementation tasks, *with a focus on Increment 1; target completion dates for measuring progress; and an approach to resourcing the JIE*. These Implementation tasks are driven by operational and fiscal realities and reflect the aggressive approach DoD is taking to implement the JIE. JIE planning will be included in future budget submissions.

JIE Increment 1 Implementation Tasks

DoD leadership has established and is tracking JIE implementation tasks that address diverse key categories that include Network Consolidation, Security, Enterprise Services, Application Rationalization, Enterprise Licensing, and Installation types (e.g., Core Data Centers, Enterprise Operations Centers, etc.). Much of the Increment 1 effort focuses on delivering and implementing reference and solution architectures and artifacts, developing TTPs needed to operate JIE capabilities (with global instantiation), defining and establishing an initial set of enterprise services, and establishing the governance processes critical to JIE management. Specific JIE Increment 1 implementation tasks for each Military Service (with delivery dates) are listed in Figure 2.

Those tasks in Figure 2 with an Area of Service (AOS) identified as Regional will only be applied to the EUCOM / AFRICOM AOR, during Increment 1. Similar implementation tasks will be established for PACOM and CONUS during Increments 2 and 3 respectively. Those tasks with an AOS identified as Global apply to all regions and should be accomplished globally by all Components even during the Increment 1period.

Figure 2. JIE Increment 1 Implementation Tasks

Category	AOS	Army / Navy / Marine Corps / Air Force Tasks	NLT Date
Network Consolidation (All)	Global	Physically Consolidate the number of Military Service networks utilizing the JIE standards and specifications/solution designs	4Q18
		Migrate all internet-facing systems to DMZs and separate applications or databases from these internet-facing systems	3Q14
	Regional	Migrate all European networks to MPLS	4Q15
Security (All)	Global	Complete SIPR PKI tokens to all of your SIPRNET users	2Q14
	Regional	Implement JIE Single Security Architecture at each installation consistent with JIE solution designs for NIPR and SIPR	4Q15
Enterprise Services (All)	Global	Utilize the Enterprise Directory Services (plan due NLT 15 May)	2Q14
		Utilize Enterprise Services or provide justification for non-compliance	2Q14
Application rationalization (All)	Global	Deliver your plan to rationalize each Military Service's applications. Report on total number of applications you have, which ones will be virtualized and moved into a Data Center, which ones will move into an IPN as legacy, and which ones will sunset immediately.	1Q14
Enterprise Licensing (All)	Global	Identify all Enterprise Licensing agreements	4Q13
Installation types (Army)	Global	Consolidate Data Centers IAW Military Service Plans; Revise plans to incorporate only one DC as an IPN on an installation.	4Q15
	Regional	Stand up 1 CDC, 3 IPNs, 10 ISNs, 42 GSU, 1 HD	4Q13 – 10 ISNs 4Q14 – 3 IPNs, 10 ISNs, Europe HD, 14 GSUs 4Q15 – 14 GSUs 4Q16 – 1 CDC (Del Din), 14 GSUs
Installation types (Navy)	Global	Establish Data Centers consistent with FDCCI plan	4Q15
	Regional	Stand up 2 IPNs, 3 ISNs, 14 GSUs	4Q14 – 1 IPN 4Q15 – 1 IPN, 3 ISNs, 7 GSUs 4Q16 – 7 GSUs
Installation types (Marine Corps)	Global	Establish Data Centers consistent with FDCCI plan	4Q15
	Regional	Stand up 1 EOC, 1 GSU	4Q14 – 1 GSU 4Q16 – 1 EOC
Installation types (Air	Global	Establish Data Centers consistent with FDCCI plan	4Q15
	Regional	Stand up 6 IPNs, 17 ISNs, 28 GSUs	4Q14 – 3 IPNs, 6

Force)			ISNs 4Q15 – 3 IPNs, 4 ISNs 4Q16 – 6 ISNs

Category	AOS	DISA Tasks	NLT Date
Network Consolidation	Global	Physically Consolidate the number of networks utilizing the JIE standards and specifications/solution designs	4Q18
		Migrate all internet-facing systems to DMZs and separate applications or databases from these internet-facing systems	3Q14
	Regional	Migrate the GIG in Europe to MPLS	4Q15
Security	Global	Issue SIPR PKI tokens to all of your SIPRNET users	2Q14
	Regional	Implement the JIE Single Security Architecture components at each installation consistent with JIE solution designs for NIPR and SIPR	4Q16
Enterprise Services	Global	Sustain Enterprise Services in DISA Catalog	4Q13
		Deliver additional Enterprise Services as identified in the JIE IMS (ABAC based Identity and Access Management, Enterprise File Storage, Records Management, Enterprise Cross Domain Services) on NIPR and SIPR.	4Q15
Application rationalization	Global	Deliver your plan to rationalize Joint applications. Report on total number of applications you have, which ones will be virtualized and moved into a Data Center, which ones will move into an IPN as legacy, and which ones will sunset immediately.	1Q14
Installation types	Global	Establish Data Centers consistent with FDCCI plan	4Q15
	Regional	Stand up 1 CDC, 1 EOC	4Q13 – 1 EOC, 1 CDC
Enterprise Licensing	Global	Identify all DISA/DoD Enterprise Licensing agreements under the purview of DISA	4Q13

Note: Regional = JIE Increment 1 tasks for EUCOM and AFRICOM

Implementation Guidance

The Department will utilize existing DoD Component programs, initiatives, technical refresh plans, acquisition processes, and funding to deploy and migrate the existing infrastructure to the JIE standards. In order to accelerate implementation of JIE Increment 1 and Future Increment Global activities, and thereby enable migration to the JIE as rapidly as possible, the Components must fund and otherwise apply resources to the efforts identified in Figure 2, which will help achieve the characteristics identified above in Section A(1).

APPENDIX A – ACRONYM LIST

ADM	Acquisition Decision Memorandum
AFNET	Air Force Network
AKO	Army Knowledge Online
AOR	Area of Responsibility
BCA	Business Case Analysis
B/P/C/S	Bases, Camps, Posts, and Stations
C2	Command and Control
C4	Command, Control, Communications, and Computers
CAC	Common Access Card
CANES	Consolidated Afloat Network and Enterprise Services
CC/S/A	Combatant Commands, Services, and Agencies
CCA	Clinger Cohen Act
CCMD	Combatant Command
CDC	Core Data Center
CDES	Cross Domain Enterprise Service
CIO	Chief Information Officer
COI	Community of Interest
CONOPS	Concept of Operations
CONUS	Continental United States
CYTAC	Cyberspace Training Advisory Council
DAB	Defense Acquisition Board
DCO	Defense Connect Online
DEE	Defense Enterprise Email
DEPS	Defense Enterprise Portal Service
DIL	Disconnected Intermittent or Low [bandwidth or connectivity]
DISA	Defense Information Systems Agency
DoD	Department of Defense

DKO	Defense Knowledge Online
DMDC	Defense Manpower Data Center
EA	Enterprise Architecture
EASF	Enterprise Application Service Forest
EDS	Enterprise Directory Service
EFD	Enterprise File Delivery
EFS	Enterprise File Sharing
EOC	Enterprise Operations Center
EXCOM	Executive Committee
EXORD	Execution Order
FDCCI	Federal Data Center Consolidation Initiative
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GCDS	Global Content Delivery Service
GEOC	Global Enterprise Operations Center
GIG	Global Information Grid
HD	Helpdesk
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
IaaS	Infrastructure as a Service
ICD	Initial Capabilities Document
IdAM	Identity and Access Management
IdSS	Identity Synchronization Service
IOC	Initial Operational Capability
IPL	Integrated Priority Lists
IPN	Installation Processing Node
ISN	Installation Service Node
IT	Information Technology

ITESR	IT Enterprise Strategy and Roadmap
JCIDS	Joint Capabilities Integration and Development System
JFC	Joint Force Commander
JIE	Joint Information Environment
JOSG	JIE Operational Sponsor Group
JROC	Joint Requirements Oversight Council
JS	Joint Staff
JTSO	JIE Technical Synchronization Office
JUONS	Joint Urgent Operational Needs Statements
KPP	Key Performance Parameter
MAS	Mobile Application Store
MDA	Milestone Decision Authority
MDM	Mobile Device Management
MPLS	Multi-Protocol Label Switching
NDAA	National Defense Authorization Act
NDU	National Defense University
NIPRNET	Nonsecure Internet Protocol Router Network
NGEN	Next Generation Enterprise
NICE	National Initiative for Cybersecurity Education
NNT	Network Normalization and Transport
NSA	National Security Agency
Ops	Operations
PaaS	Platform as a Service
PCC	Planning and Coordination Cell
PE	Program Element
POA&M	Plan of Actions and Milestones
POR	Program of Record
SIPRNET	Secret Internet Protocol Router Network
SOP	Standard Operating Procedure

SSA	Single Security Architecture
STAX	Infrastructure as a Service/Platform as a Service (DISA service offering)
TTPs	Tactics Techniques and Procedures
UC	Unified Capabilities
UCP	Unified Command Plan
USAFRICOM	United States Africa Command
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
USEUCOM	United Stated European Command

APPENDIX B – LIST OF FIGURES