The Department of Defense Strategy for Implementing the Joint Information Environment

September 18, 2013

The estimated cost of report or study for the Department of Defense is approximately $27,000 for the 2013 Fiscal Year. This includes $14,000 in expenses and $13,000 in DoD labor.

Generated on 2013Sep18 RefID: 0-2F91712

This page intentionally left blank.

The Department of Defense Strategy for Implementing the Joint Information Environment (JIE)

Response to Section 931(a) of the Fiscal Year 2013 National Defense Authorization Act (NDAA)

Table of Contents

Executive Summary

Increasingly Department of Defense (DoD) mission success depends on the ability of military commanders and civilian leaders to act quickly and effectively based on the most accurate and timely data available. In today's national security environment, it is imperative that DoD resolve barriers to trusted information sharing and collaboration, within the Department and with DOD's mission partners, to provide better access to information, and to enhance the nation's effectiveness to defend against cyber threats and vulnerabilities. And DoD must achieve this in a fiscal environment that demands reduced Information Technology (IT) infrastructure costs.

For this reason, the DoD has undertaken an ambitious, multi-year IT modernization effort to achieve the Joint Information Environment (JIE). This effort will realign, restructure, and modernize how the Department's IT networks and systems are constructed, operated, and defended. JIE will consolidate and standardize the design and architecture of the Department's networks. Since JIE is not a Program of Record, it should be noted that 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.

While this report highlights a number of anticipated benefits to achieving JIE, most notable is enhanced data access and information sharing within the Department and with appropriate federal, state, international, and other partners. Additionally, JIE will facilitate faster development and deployment of new warfighting support capabilities, including software applications. Other anticipated benefits from JIE include:

- Improved mission effectiveness
- More effective training
- Increased cyber security
- Optimized resources and IT efficiencies

This report outlines the DoD strategy for JIE implementation with the following topics and sections:

Vision and Roadmap: The vision of JIE is to ensure that DoD military commanders, civilian leadership, warfighters, coalition partners, and other non-DoD mission partners have access to information and data provided in a secure, reliable, and agile DoD-wide information environment. Mission assurance for warfighter needs is integral to DoD's vision for JIE – the Department is working to provide more convenient, assured, and ready access to information on a wider range of devices, under widely diverse conditions. This vision is spelled out in a roadmap that discusses both operational and technical characteristics, with a focus on the following technical characteristics: Single Security Architecture, Federated Networks, Identity and Access Management, Data Center Consolidation, Software Application Rationalization and Server Virtualization, Desktop Virtualization and Thin-Client Environments, Mobility Services, and Enterprise Services.

DoD IT operations that support warfighter, business operations, and intelligence information are currently limited by Component-centric, non-standardized, non-integrated and non-interoperable

capabilities. The JIE will enable DoD network operators and defenders to work as a more unified team. For example, it will enable network, system operators, and defenders at multiple levels to have visibility of systems and networks across the Department, as well as allow commonality in how cyber threats are encountered. This means DoD 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.

Key Milestones, Metrics, and Resources: Achieving JIE means fundamentally changing how DoD implements, operates, and defends its IT assets. While the Department will continue to utilize common operational tactics, techniques, and procedures (TTPs) to implement JIE, it must address emerging management and governance issues related to a new operating environment. To that end, JIE implementation is being addressed in a phased approach with key milestones and metrics for measuring progress. These phases, or "increments," address myriad key elements that keep leadership informed on overall changes to DoD IT infrastructure and provide updates on how implementation is progressing. These elements include planning, implementation, transition, operations, and defense. The JIE approach focuses on general changes to the IT infrastructure and work across the Department with an initial instantiation in the European and Africa geographic regions. As those changes are tested and validated, the Department will make decision on the scope of future increments, with an interest in expanding efforts in the Pacific Region as a major focus of the next increment.

From a user perspective, as milestones are met, resources applied, and outcomes measured, the JIE should be analogous to a utility – always available when and where the user needs it. For example, it will enable a single set of applications across DoD for like services, a standardized architecture and a robust and resilient infrastructure, common operational TTPs, agile DoD-wide help-desk user support, a highly trained workforce, and standardized roles and responsibilities at each operational level. This dynamic combination will create a seamless, DoD-wide information environment.

Acquisition Strategy and Management Plan: In order to achieve this ambitious, comprehensive IT modernization effort and reap the operational and fiscal benefits of JIE, senior-leadership engagement and strong governance structures and processes are essential. The Department will evaluate JIE progress by considering its impact from a warfighter mission-focused perspective. Specifically, Operational Effectiveness Objectives and associated Performance Measures will measure improvements in overall operational effectiveness, supporting these objectives.

The DoD CIO has primary responsibility for developing and enforcing DoD's overall IT policy, architecture, and standards, and the Components are accountable for implementing and complying with DoD CIO direction. Both the DoD CIO and Component CIOs are responsible for overseeing IT investment management and information assurance (IA) in compliance with the Clinger-Cohen Act (CCA) and the Federal Information Security Management Act (FISMA). The DoD CIO will leverage the DoD CIO Executive Board (EB) and its reporting relationship to the Deputy's Management Action Group (DMAG) as the focal point for DoD IT effectiveness and modernization. The CIO EB will serve

as the DoD's senior functional oversight forum, where IT effectiveness and modernization matters are vetted for input to planning, programming, budgeting, and execution (PPBE); the Defense Acquisition System (DAS); and the DMAG for approval. Components will submit their aligned IT effectiveness implementation plans to the DoD CIO EB, and their progress will be tracked, consolidated, and briefed to the DMAG.

Key Technical and Policy Challenges: Efforts to achieve JIE are moving DoD from its current organization-centric, networks-and-services construct toward an operationally focused, information-centric construct. This fundamental shift to a more enterprise approach will enable the joint warfighter to focus more on obtaining the information for decisions about mission objectives and to focus less on being the capability integrator. When fully achieved, the JIE will ensure that the warfighter at the tactical-edge is equipped with a single, joint infrastructure by integrating previously stove-piped structures. This clear shift in approach demands new policies to support both technical changes as well as policy and cultural changes.

Achieving the JIE involves developing and consistently implementing new technical capabilities on an unprecedented scale that will touch virtually every organization within the Department. As discussed in detail in this strategy for implementing the JIE, the following technical areas are particularly complex:

- ***Single Security Architecture (SSA)*** – Establishing an SSA will collapse network security boundaries; reduce the Department's external attack surface; enable better containment and maneuver in reaction to cyber attack; and standardize management, operational and technical security controls.

- ***Network Normalization*** – DoD's current system of disparate network, processing, and storage infrastructures impedes internal and external collaboration for the warfighter and mission partners. As such, a foundational aspect of achieving the JIE is to provide a single, protected information environment that securely, reliably, seamlessly interconnects warfighters.

- ***Identity and Access Management*** – Optimized Global Identification, Authentication, Access Control, and Directory Services are central to satisfying the warfighter's need for a portable identity and the ability to share contact information between organizations.

- ***Enterprise Services*** – An enterprise service is a service, like email, that is provided in a common way across the Department, and is provided by a single organization acting as the enterprise-service provider. DoD is emphasizing development and deployment of enterprise services as part of JIE that are designed to operate in deployed, disconnected, or low-bandwidth information environments.

- ***Cloud Computing*** – DoD's move to cloud computing presents challenges, especially in the management of thousands of shared computer servers, cyber security (as part of single security architecture), resilience and failover, and migration of software applications onto the cloud.

- ***Data Center Consolidation*** – The DoD will continue to consolidate computing power by closing and consolidating data centers across the Department, while concurrently identifying existing data centers to be transitioned into JIE Core Data Centers (CDCs). Data center consolidation will be integral to facilitating the move the Department to a standardized computing architecture.

Capability Gaps and Dependencies: Numerous Joint Capabilities Integration and Development System (JCIDS) documents describe the gaps and capability requirements that the JIE strives to address. In particular, the JIE Initial Capabilities Document (ICD), currently in coordination, is the capstone document that defines the capabilities that will serve as the foundation for continuous improvement and performance optimization of the JIE. These capabilities will provide enterprise-level solutions that close identified gaps for information sharing, which include the DoD Components; Intelligence Community; U.S. Government agencies; allies; and other mission partners, such as industry organizations and Non-Governmental Organizations (NGOs). This Implementation Plan discusses in further detail issues surrounding dependencies, specifically those related to Data Center Consolidation; Enterprise Services; Network Normalization and Consolidation; and Governance and Oversight.

Personnel Challenges: As the DoD is developing and implementing JIE, it also must transition and transform its workforce to ensure that it can better structure, operate, and defend its information, networks, systems, services, and capabilities in order to achieve operational and strategic advantage. The Department needs highly skilled IT managers who can govern the JIE, as well as operational personnel who can communicate and coordinate across DoD Component command structures to conduct offensive, defensive, and sustainment missions. To achieve this goal, DoD must recruit and retain qualified individuals with the necessary competencies and skills, and provide them with requisite training, certification, and developmental opportunities. Effective workforce transformation will ensure that the DoD can structure, operate, and defend its information, networks, systems, services, and capabilities. Personnel-related challenges specific to implementing the JIE discussed focus on both civilian and military personnel, cyber workforce development, and training and certification.

A. Discussion

Section 931 of the Fiscal Year 2013 National Defense Authorization Act (NDAA) directs the Department of Defense (DoD) to submit to Congress a strategy to implement the Joint Information Environment (JIE). In response to this requirement, this report explains in the following sections *how the Department will implement JIE* by addressing the below six statutorily defined topics:

- Vision and Roadmap
- Key Milestones, Metrics, and Resources
- Acquisition Strategy and Management Plan
- Key Technical and Policy Challenges
- Capability Gaps and Dependencies
- Personnel Challenges

As background on why JIE implementation is vital to the Department, *increasingly, DoD mission success depends* upon the ability of military commanders, civilian leaders, and mission partners to act quickly and effectively, *based on the most accurate and timely data and information available*.

Recognizing information as strategic asset, DoD is undertaking a realignment, restructuring, consolidation, and standardization effort that addresses how its Information Technology (IT) networks, systems, and services are constructed, operated, and defended. This effort includes:

- Optimized Networks
- Secure, Defendable, Redundant, Resilient Environment
- Open Architecture
- Shared IT Infrastructure and Enterprise Services – including Service-provided, Mission-unique Capabilities
- Identity Access Management (IdAM)

JIE is a framework for DoD IT modernization. JIE is design and architecture to consolidate and standardize the Department's networks. It consists of overarching architectures, standards, and specifications; common ways of operating and defending; and common-engineered solution designs implemented across the Department. DoD will utilize existing Component programs, initiatives, and technical refresh plans to deploy and migrate the existing infrastructure to the JIE standards, utilizing specific implementation guidance – from a DoD-wide perspective. It is not:

Myriad benefits to the Department are anticipated from the JIE. It will enable enhanced data access and information sharing within the Department and with appropriate federal, international, and other partners. In addition, JIE will facilitate faster development and deployment of new warfighting support software applications. Additional anticipated benefits from JIE include:

- Improved mission effectiveness
- More effective training
- Increased cyber security
- Optimized resources and IT efficiencies

It is intended to ensure that services are not duplicated and that the command and control of these services align under a single C2 structure guided by the principle of unity of command.

A(1) Vision and Roadmap

Introduction

The Department intends to provide a *secure, reliable, and agile DoD-wide information environment* for use by the Joint forces and non-DoD mission partners across the full spectrum of operations.

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 will empower DoD users with the following:

- 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 DoD-wide help desk user support
- Highly trained workforce

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, regardless of its service provider or use* – such as mission-specific utilization – and it will use common TTPs developed at the enterprise level, which will improve security.

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

- Single Security Architecture
- 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

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 – and Department-level consolidation of data centers and network operations centers operating under a single security architecture. 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 offering, and will 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 include reducing and flattening the complexity and cost of network defense; improving DoD's security posture and support for mobile, embedded, and other users; decreasing operational duplications; and establishing joint protections and responsibilities across Community of Interests (COIs). In addition, SSA will enable DoD to overlay COIs on the network across multiple regions; support non-traditional users, such as those that are mobile or embedded; and increase effectiveness by improving interoperability and information sharing. Finally, SSA will increase DoD's network security by separating server computing and traffic from end-user devices; dividing the network into manageable, securable zones that enforce consistent policies; placing sensors at the most efficient locations for traffic capture and inspection; and supporting the centralization and consolidation of the operations centers, tools, and personnel that operate and defend the network.

Optimized Networks, i.e., reducing the number of networks, will allow the sharing of resources among multiple independent networks. For example, these optimized networks will enable expanded use of a shared IT infrastructure and enterprise services, thin-client end-user technologies, unified communications, email, and cloud computing services at DoD. Anticipated benefits of this sharing and optimization include optimizing resource usage, improving the quality of network-based services, reducing both manpower and the complexity of networks, and reducing costs.

Identity and Access Management (IdAM) is fundamental to the security of data and secure information sharing with mission partners. 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 both the security of the DoD's IT while also increasing mission effectiveness. This capacity, combined with access-based controls, will allow person and non-person entities to securely access authorized DoD information, anywhere, at any time.

This new expanded approach will update the current manually intensive, inconsistent, time-consuming and resource-heavy local administrative 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 will include capabilities that completely automate the generation of user accounts based on Nonsecure Internet Protocol Router (NIPRNET) common access cards (CACs) and Secrete Internet Protocol Router Network (SIPRNET) tokens, and make real time information access control decisions based on requesting user attributes, such as clearance, rank, and job function. More effective monitoring and attribution 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.

Data Center Consolidation is critical to improving DoD-wide efficiencies. As context, in fiscal 2014, DoD had about 2,000 data centers, and the consolidation goal for fiscal 2017 is to reduce to less than 500 data centers organized into four tiers of capability. The current array of DoD data centers, networks, and systems introduces unnecessary costs, constrains interoperability, and introduces 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, and ensure 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.

An important element of the effort to consolidate DoD's data centers is the JIE Core Data Center (CDC) initiative. 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. In addition, the DoD Data Center Reference Architecture ensures that data centers that will be type classified, and governed through investment review processes at Component and Department levels.

Software Application Rationalization and Server Virtualization will enable additional IT efficiencies and enhance information sharing. For example, increased application virtualization will reduce costs for facilities maintenance and operations, as well as for server operations and maintenance, and will improve automation for server management and provisioning. DoD Components are currently rationalizing, normalizing, standardizing, and, to the extent possible, virtualizing the software applications and hardware used by the Department and hosted in data centers. This 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.

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 are already in limited use across the Department; over time, the JIE will further extend, accelerate, and standardize their implementation. In addition, the virtual desktop environment is a critical piece of the Department's mobility strategy. Its widespread use will enable users to access their computing environments – hosted in a JIE CDC – from any thin client or mobile device, from any DoD location. Likewise, users also can access their information and applications from DoD-approved tablets, pad computers, or Smartphones.

Mobility Services are an integral component of the JIE communications and networking architecture. The application of mobile technology into JIE operations; the integration of secure and non-secure communications; and the development of portable, cloud-enabled command and control capability will dramatically increase the number of people able to collaborate and share information rapidly. JIE infrastructure will support unclassified and classified commercial mobile devices, institute mobile device policies, and provide software distribution for the Department's mobile applications. The DoD Mobile Strategy and Commercial Mobile Device (CMD) Implementation Plan outlines the initial execution approach to JIE Mobility capability.

Enterprise Services are services, like email, that are provided in a common way across the Department, and are provided by a single organization acting as the enterprise service provider. Enterprise Services that range from critical business office functions to enterprise applications supporting cross-functional missions have been identified by the Department as customer-facing and infrastructure Enterprise Services. These will serve as the basis of 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, and Enterprise File Delivery; however, final approval and implementation specifics are still being determined. The Defense Information Systems Agency (DISA) is currently providing the candidate Enterprise Services that support customer-facing capabilities, machine-to-machine services, and infrastructure services. These enterprise services will be located inside DoD Core Data Centers; additional enterprise services are being planned.

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 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 still will be operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common TTPs.

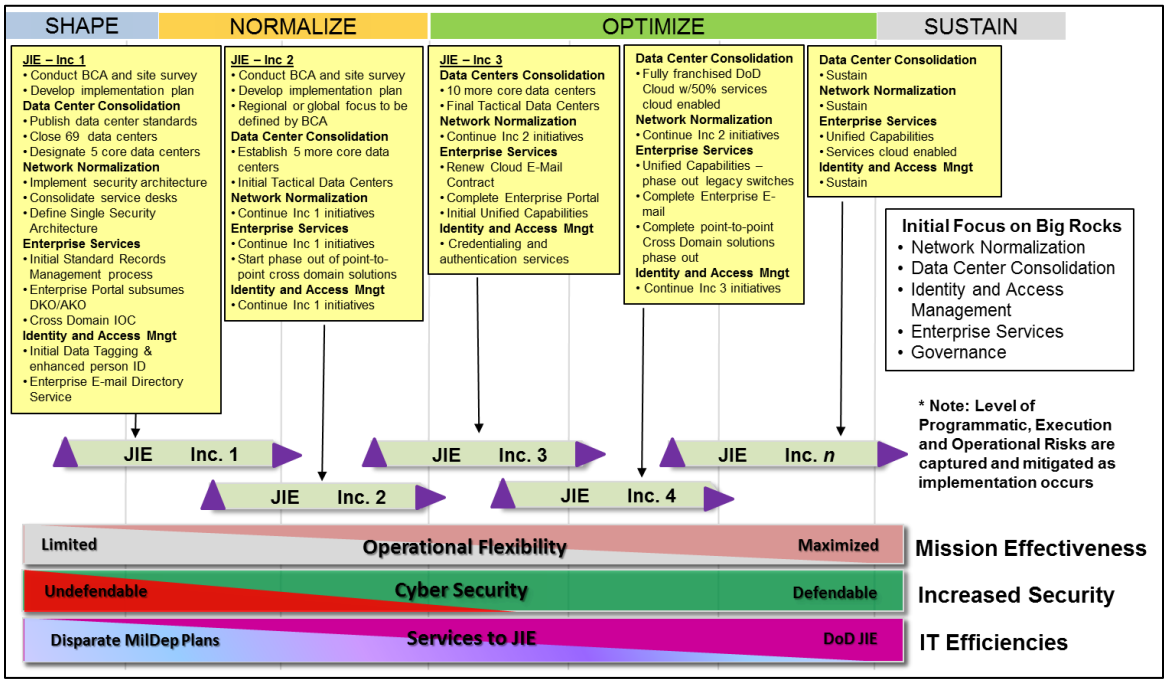
A(2) Key Milestones, Metrics, and Resources

Introduction

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 initially planned JIE approach incorporated incremental implementations layered on top of budgeted IT modernization of its IT infrastructure. Due to complexity, scope, and budgetary constraints, the Department scoped Increment 1 to focus on changes in the European region. This approach will help validate the concepts prior to executing detailed planning and future implementation plans. Table 1 below depicts the initial plan.

Table 1. JIE Roadmap



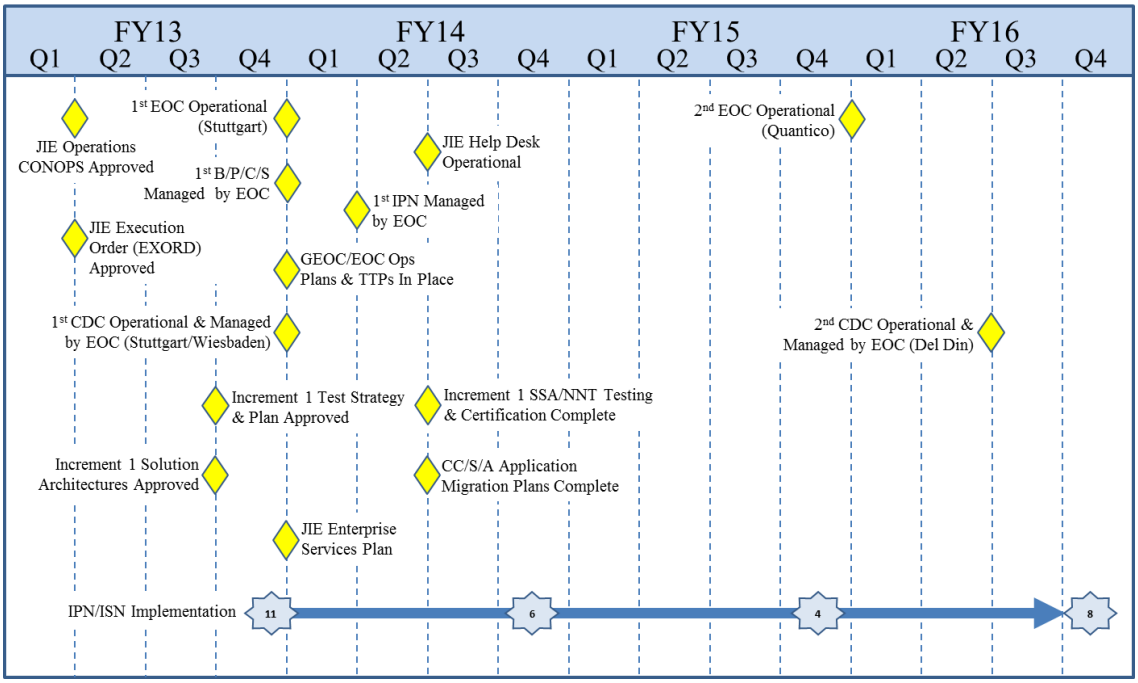
Therefore, this section outlines for JIE implementation *key milestones, with a focus on Increment 1; metrics for measuring progress; and an approach to resourcing the JIE*. These milestones are driven by operational and fiscal realities and reflect the aggressive approach DoD is taking to implement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

Key Milestones – JIE Increment 1

DoD leadership has established and is tracking milestones that address diverse key areas that include

planning, implementation, transition, operations, and defense. As depicted below in Table 2, Increment 1 focuses on delivering and implementing reference and solutions 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.

Table 2. JIE Increment 1 Key Milestones



**Note: Milestones listed on this chart are illustrative and may not match current planning in the JIE Integrated Master Schedule.

Global implementation of JIE Increment 1 focuses on the European region, and it supports the mission areas of United States European Command and United States Africa Command. *This approach maintains a global focus, while allowing 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.

Further, key milestones for the JIE Increment 1 are illustrated above in Table 2. DoD continues to revise and refine its plans for Increment 1; therefore, the information provided in this table represents a *snapshot in time that will be updated as implementation planning and execution proceeds*. Selected milestones, including those accomplished or in progress, also will be discussed further in this section. JIE implementation milestones that have been accomplished or are in progress include:

- ***JIE Execution Order (JIE EXORD)***: On 29 November 2012, the Secretary of Defense approved the JIE EXORD, which provides organizations within the Department with their initial instructions for JIE planning and implementation execution.

- ***JIE Operations Concept of Operations (JIE Ops CONOPS)***: On 25 January 2013, the DoD JIE EXCOM approved the JIE Ops CONOPS, which describes roles, responsibilities, organizational relationships, functions, and tasks necessary to successfully operate and defend JIE.

- ***JIE Enterprise Architecture (JIE EA)***: The DoD Chief Information Officer (CIO) developed the JIE EA to provide the Operational Concept, Functional Overview, Security, and to-be architecture of JIE. It is currently being reviewed within DoD Components.

- ***JIE Management Construct and Charter***: DoD CIO issued a JIE Management Construct and Charter on 9 November 2012 to manage, guide, and prioritize the JIE efforts. *The JIE Management Construct is the Department's primary mechanism for engaging with key stakeholders* within DoD, across government, with mission partners, and with industry to further define and implement the JIE framework in accordance with the implementation strategy described in this report.

- ***JIE Technical Synchronization Office (JTSO)***: A Joint Chiefs of Staff (JCS) memorandum on 9 August 2012 established the JTSO. Led by DISA, in close coordination with the development and approval of the JIE EA, the JTSO is leading the development of more detailed solution architectures that will be used to inform and guide the development of specific solutions.

- ***JIE Operations Sponsor Group (JOSG)***: A JCS memorandum on 23 October 2012 established the JOSG. Led by USCYBERCOM, the JIE Operations Sponsor Group (JOSG) is leading the development of the operational concepts, plans, processes, and TTPs that will be used to operate and defend the JIE.

- ***JIE Increment-1Transitional CONOPS***: The DoD JIE EXCOM approved the JIE Increment - 1 Transitional CONOPS on 25 July 13. This describes roles, responsibilities, organizational relationships, and functions necessary for JIE Increment-1 to include the initial Enterprise Operations Center (EOC)'s ability to successfully operate and defend the JIE and address the early transition towards the end-state described in the 25 January 2013 JIE Ops CONOPS.

- ***Enterprise Operations Centers (EOC)***:

    - DoD stood up the first EOC in Stuttgart, Germany on 31 July 2013.
    - USCYBERCOM will lead the establishment an initial Global Enterprise Operations Center (GEOC) capability later this year.

- Both facilities will fully leverage existing facilities and capabilities, and will validate the operational concepts of operating and defending the DoD Networks.

The initial list of activities/milestones that will support long-term implementation of JIE are outlined in the table below.

Table 3. JIE Future Increment Global Activities

Category	Task	Completion (Est.)
Network Consolidation	• Physically consolidate the number of Service networks utilizing the JIE standards and specifications/solution designs • Migrate all Internet-facing systems to DMZs, and separate applications or databases from these Internet-facing systems	4QFY18 3QFY14
Security	• Issue SIPRNET PKI tokens to all DoD Component SIPRNET users	2QFY14
Enterprise Services	• Utilize the Enterprise Directory Services (plan due NLT 15 May 2013) • Utilize Enterprise Services or provide justification for noncompliance • Sustain Enterprise Services in DISA Catalog • Deliver additional Enterprise Services as identified in the JIE IMS on NIPRNET and SIPRNET, including: o ABAC based Identity and Access Management o Enterprise File Storage o Records Management o Enterprise Cross Domain Services	2QFY14 2QFY14 4QFY13 4QFY15
Application Rationalization	• Deliver a plan to rationalize Service and Joint applications; report on the total number of applications that will be virtualized, that will move to an CDC or IPN, or that will sunset or be retired immediately	1QFY14
JIE Node Transition	• Establish CDCs consistent with the Federal Data Center Consolidation Initiative (FDCCI) plans and JIE objectives	4QFY15
Enterprise Licensing	• Identify all Enterprise Licensing agreements	4QFY13

Metrics

DoD recognizes that measuring progress is a critical aspect of any undertaking, especially one the scope and size of the JIE. *The Department will evaluate JIE progress by considering its impact from a warfighter mission-focused viewpoint*. A set of Operational Effectiveness Objectives will focus these efforts. Additionally, Performance Measures, still in development, will measure improvements

in overall operational effectiveness and security, supporting these objectives. These objectives are provided below at Table 4. As the JIE continues to mature and new capabilities are identified and implemented, the initial set of objectives described below are anticipated to also change and mature.

Table 4: JIE Operational Effectiveness Objectives

Optimize effectiveness for the commander	• JIE supports the Joint Force Commander's (JFC) cyber operations plan
	• Enterprise services and service-unique applications required for operations are available during any contingency
	• JFC has secure, assured communications with mission and coalition partners
	• Ensuring that the commander:
	  ○ Can achieve desired operational effect
	  ○ Has access to required information and services
	  ○ Can conduct operations in a degraded JIE

Optimize C2 of the DoD GIG Operations and Defensive Cyber Operations	• Commander and supporting Enterprise Operations Center (EOC) can defend against malicious cyber activity by directing response actions and contingency plans • Mission success is enabled with minimal complexity and friction, while operational continuity and understanding are maintained • Mission-critical decisions are enabled that result in effective responses that accommodate direction change without detracting from the primary mission

Provide situational awareness of operational status and cybersecurity status of the JIE	• Single Security Architecture (SSA) sensor status is visible at Global Enterprise Operations Center (GEOC) and EOC
	• EOC can monitor and manage configuration changes to the JIE to ensure its health and integrity. These activities include:
	  ○ Enterprise Services Management
	  ○ Network Management
	  ○ Satellite Communications Management
	  ○ Electromagnetic Spectrum Management
	• Aggregate performance data from the networks, systems, applications, and enterprise services comprising the JIE is visible in the GEOC and EOC
	• Automated reporting of DoD information network configurations and vulnerability status to the GEOC and EOC from the base, post, camp, and station (B/P/C/S)

Optimize Security/Cyber defensibility of DoD information networks	• JIE is protected by an SSA
	• EOC can effectively:
	  ○ Execute passive defense of DoD networks at all echelons by automating the management and execution of DoD and United States Cyber Command (USCYBERCOM) policies and preplanned courses of action
	  ○ Defend networks in cyber real-time by activating rule sets to defeat cyber-attacks via the SSA
	  ○ Automatically ID weak systems, ascertain configurations, and determine operational risk from improper configurations and unpatched systems
	  ○ Rapidly reconfigure networks to thwart advanced persistent cyber threats to ensure mission integrity and continuity

Resources

Given the size and complexity of the DoD infrastructure as well as the phased implementation, assessing the lifecycle costs and savings related to JIE is a highly complex exercise. Assessment work on these issues continues. As with most transformational efforts, initial activities may require some investment. Since JIE is not a Program of Record (POR), it should be noted that 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. An organizational construct for coordinating implementation planning, establishing master schedules, and proposing options and alternatives, in conjunction with impacted PORs, will be needed to synchronize actions across organizational and program element lines. The Department will continually assess current and future IT-based initiatives against JIE-related concepts, architectures, standards, and TTPs to inform, align and drive future investments.

A(3) Acquisition Strategy and Management Plan

Introduction

This section *outlines the Department's approach to acquisition, integration, compliance, and management in support of JIE implementation*. The DoD Chief Information Officer (CIO) is charged with making Department-level recommendations on IT-related policy and IT acquisition decisions that will support the JIE initiative. Governance and senior leadership engagement will be critical to the successful implementation of the JIE's capabilities.

Acquisition Strategy

As noted earlier, the JIE is not an acquisition program. This is an IT modernization effort that will consolidate, standardize, and optimize the design and architecture of the DoD's networks. To facilitate implementation of JIE through acquisition across the Department, it is important to note that new IT programs will require compliance 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 myriad means by which acquisition programs can be influenced. *Because no single approach can address the full range of objectives for the JIE, a variety of approaches are being 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

enterprise-level hardware/software acquisitions. 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.

Integration

The JIE will provide program offices with an integrated "platform" of network computing, core enterprise services, and security at a specified, testable, and guaranteed level of performance, allowing them to focus on mission-support applications. This integrated platform will replace today's disparate IT infrastructures and architectures that result in IT programs developing and integrating the entire IT "stack," to include:

- Network and computing services
- Computers and mobility devices
- Standard software loads on the computers and servers
- Core machine-to-machine services, like messaging
- Global load balancing

In addition, the program must integrate cybersecurity across all of this, from operating system configuration, to access controls, to perimeter defenses, to cyber intrusion detection and diagnosis.

DoD will speed up the development, testing, and cyber security compliance of programs and systems by standardizing software development environments and integrating test and security evaluation capabilities that match the production platform. *Programs will deliver faster and will inherit better cybersecurity*.

Compliance

The DoD CIO will mandate compliance with the JIE Enterprise Architecture (EA). *This compliance will be assessed annually* in concert with program design reviews, acquisition milestone reviews, business systems investment reviews, and other programmatic decision points at the delegated organization or level. Architecture compliance for the JIE will initially focus on those areas that are well defined and documented, such as the components of SSA, but will be expanded as other areas mature. Compliance enforcement will be the responsibility of acquisition oversight organizations and Milestone Decision Authorities (MDAs), and Investment Decision Authorities in the Department.

In addition to this architectural compliance, operational compliance also must take place. *The JIE is making fundamental changes to the ways that the DoD operates and defends it networks*. The approved JIE Ops CONOPS provides a basis for this operational compliance. Existing program reviews and milestone decisions also will incorporate operational compliance assessments. Other mechanisms for influencing and guiding DoD IT acquisitions and compliance that will be implemented are outlined below in Table 5.

Table 5: Mechanisms for Influencing DoD IT Acquisitions

Mechanism	Implementation	Benefits
Acquisition Decision Memorandum/Defense Acquisition Board (ADM/DAB)	Incorporate JIE mandates for specific programs into program ADMs and enforce through DABs	Provide a strong way for identifying and enforcing JIE requirements for major programs.
Interoperability Key Performance Parameter (KPP)	Update the existing interoperability KPP to incorporate JIE interoperability requirements	Meeting a KPP is a hard and fast criterion for achieving a successful program milestone decision.
Policy and Guidance	Revise and enforce policy at the DoD and Component levels detailing specific JIE compliance requirements as they are developed. Modify existing policies to remove barriers to JIE adoption.	Establish consistent mandates across DoD and provide for multiple, mutually supporting enforcement mechanisms.
Strategic IT Solution Sourcing	Set Component objectives and metrics for strategic sourcing results that are aligned with JIE objectives and require annual progress reporting.	Establish accountability for shared process improvement, cost reduction, and standardization focused on the JIE objectives.
IT Program and Procurement Visibility	Ensure budget submissions clearly identify IT investments to identify opportunities for IT efficiencies.	Provide DoD with the ability to identify IT investments beyond major programs and be common definitions enabling identification of opportunities for efficiencies.

Management Construct

To manage, guide, and prioritize the JIE, the DoD CIO issued a JIE Management Construct and Charter, in coordination with the DoD Components. *This JIE management construct is the Department's primary mechanism for engaging* with key stakeholders within DoD, across government, with mission partners, and with industry to further define and implement the JIE framework in accordance with the implementation strategy described in this report.

The ***JIE Executive Committee (JIE EXCOM)*** – jointly led by the DoD CIO, Joint Staff J-6, and the USCYBERCOM CIO/J-6 – sets the JIE direction, establishes goals and objectives, provides oversight, and maintains accountability. The JIE EXCOM also provides strategic leadership and direction to the following JIE working groups:

- ***JIE Planning and Coordination Cell (PCC)***, jointly led by the DoD CIO, Joint Staff J-6, and the USCYBERCOM CIO/J-6, is responsible for synchronizing DoD Components' actions to realize an integrated Department-wide implementation of the JIE. PCC maintains the JIE

Integrated Master Schedule (IMS); tracks implementation plans; coordinates activities among governance, operations, and the JTSO; and manages implementation issue resolution and execution.

- ***JIE Operations Sponsor Group (JOSG)**, led by USCYBERCOM,* develops, integrates, and synchronizes operational tasks and procedures in support of the JIE that are integrated with existing Department-level procedures. JOSG works closely with the JIE theater-level execution sponsors, and coordinates and leads the development of operational CONOPS, TTPs, and Standard Operating Procedures (SOPs). It also identifies and makes recommendations on budgetary priorities necessary to support JIE operations, in coordination with Combatant Command (CCMD) Integrated Priority Lists (IPL) and cyber component inputs.

- ***JIE Technical Synchronization Office (JTSO)***, led by DISA, serves as the technical and implementation lead for the JIE, and provides engineering and architecture direction. It works to realize an integrated, DoD-wide implementation of the JIE by developing, integrating, and synchronizing the JIE technical plans, programs, and capabilities. JTSO leads the development of DoD technical specifications, designs, and standards (IAW the DISR) to enable the JIE; assesses maturity of JIE capabilities based on tests of systems, services, and products, as well as Combatant Commands, Services, and Agencies (CC/S/A) operational assessments of JIE TTPs at exercises; manages the technical portion of the Department's JIE Plan of Actions and Milestones (POA&M); and ensures that JIE security architecture development is designed to secure the infrastructure, provide access, and allow cross-environment data-sharing.

- ***JIE Governance Group***, led by the DoD CIO, is designed to align the JIE to the Department's requirements, budgeting, and acquisition processes. It is responsible for policy compliance, capability validation, resourcing, Program Objective Memorandum (POM), and budget decisions. It also provides the overarching plans, guidance, and policy that inform requirements approval and is responsible for the development of the JIE Enterprise Architecture.

A(4) Key Technical and Policy Challenges

Introduction

The Department is making fundamental and permanent shifts away from the current organization-centric, network-and-services construct in order to reach the JIE desired vision and end-state. *It is moving to an operationally focused, information-centric construct*. This new approach enables the Joint warfighter to *focus more on obtaining the information for decisions* about mission objectives and accomplishments, *and to focus less on being the capability integrator*.

The JIE vision will ensure that the tactical-edge users are equipped with a single, joint infrastructure by integrating previously stove-piped structures. This consolidated infrastructure will enhance mission effectiveness by ensuring that data is accessible and distributed across all DoD Components and mission partners, as appropriate. As discussed in this section, *this new paradigm presents significant technical and policy challenges* that the DoD is addressing; the following technical challenges have been of particular difficulty and are discussed below in detail:

- Single Security Architecture
- Network Normalization
- Identity and Access Management
- Enterprise Services
- Cloud Computing
- Data Center Consolidation

Technical Challenges

The JIE involves developing and consistently implementing new technical capabilities on an unprecedented scale that will touch virtually every organization within the Department. Of the myriad technical challenges to this initiative, the following are particularly significant to overcome:

Single Security Architecture (SSA): 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. To establish an SSA, the Department is leveraging the technical and operational expertise of the National Security Agency (NSA), Defense Information Systems Agency (DISA), and the 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 also will allow the DoD Components to remove existing redundant security suites, which will free resources, both equipment and personnel, to be repurposed and applied to fill other gaps. *The end result of establishing an SSA will be a set of capabilities that will enable DoD cyber forces to "see, inspect, block, and collect" network traffic and provide the Joint warfighter with a trusted information environment*.

***Network Normalization*:** Network normalization will reduce, standardize, and consolidate DoD's current system of disparate network, processing, and storage infrastructures, which currently are too diverse to protect and defend. This incompatible, mixed environment also impedes internal and external collaboration and places warfighters 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*. DoD is implementing network technologies like Multi-Protocol Label Switching (MPLS). This will enable the Department to protect backbone routers, segment management controls, and multiple user data streams. It will also help protect against and isolate cyber threats and contain malicious activity.

Identity and Access Management (IdAM): Optimized Global Identification, Authentication, Access Control, and Directory Services are central to satisfying the warfighter's need for a portable, non-reputable identity, and the ability to share information between organizations and authorized users. IdAM facilitates this goal, because optimization is achieved by streamlining the identity information repositories, security frameworks, and credential authorization processes, and by ensuring that identity and authorization information is available to appropriate organizational counterparts. The DoD CIO took a critical step towards realizing these capabilities by directing the DoD Components to begin using DoD Enterprise Directory Services, which provide DoD Enterprise identity and contact attributes and support people discovery across the DoD community. The granting of access to authorized information to users on an automated basis will significantly reduce the intense manpower effort required today, while improving the control to and auditability of access to information across the network. *The realization of a robust set of IdAM capabilities will provide the Joint warfighter and their supporting mission areas with secure, authorized access to all information and services required, regardless of location.* In addition, it will increase commander confidence that their units have access to mission-essential information and services while maintaining the appropriate level of security for these information assets.

***Enterprise Services*:** An enterprise service is a service, like email, that is provided in a common way across the Department, and is provided by a single organization acting as the enterprise-service provider. While current Enterprise Services are expanded to support the DoD's business processes at higher enterprise levels, there are significant challenges in extending these Enterprise Services to 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. These services must be available to consumers who function in disconnected, intermittent, or low-bandwidth (DIL) information environments. The DoD CIO will be placing additional emphasis on developing and deploying Enterprise Services as part of future increments of the JIE that are designed to operate in deployed DIL. *Providing this 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*.

Cloud Computing: DoD's move to cloud computing has challenges, especially in the management of thousands of shared computer servers, cyber security (as part of the single security architecture), resilience and failover, and migration of software applications onto the cloud. They 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
- Agile acquisition of Service and sustainment funding
- 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 IA policies and instructions, and alignment of IA controls and processes with those used across the federal government.

- DoD use of the Federal Risk and Authorization Management Program (FedRAMP) for low and moderately sensitive data; FedRAMP will establish a standard approach for assessing and authorizing cloud computing services.

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

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

***Data Center Consolidation*:** DoD will continue to consolidate computing power by closing and consolidating data centers across the Department as part of FDCCI. As context, in fiscal 2014, DoD had about 2,000 data centers, and the consolidation goal for fiscal 2017 is to reduce to about 100 data centers. DoD also will identify existing data centers to be transitioned into a limited number of JIE CDCs. Finally, DoD will accelerate efforts to normalize, rationalize, and reduce the number of the functional software applications that are in use; this will drive out duplicative and unnecessary applications that increase licensing and support costs. Adoption of cloud computing technologies must be incentivized and facilitated in smart ways that enable more effective and efficient sharing of commodity IT functions and enhance warfighter agility, survivability, and lethality.

Policy Challenges

As a different way of doing the business of IT for DoD, JIE will require changing existing policies, as well as developing new policies to account for implementation, operation, and sustainment. To *develop and implement comprehensive, useful DoD IT policies to govern the JIE*, the Department must maintain an appropriate balance across the body of federal and international law that regulates IT within DoD, (e.g., the Clinger-Cohen Act of 1996 [CCA], the Federal Information Security Management Act of 2002 [FISMA], the Health Insurance Portability and Accountability Act of 1996 [HIPPA], and the Privacy Act of 1974).

The DoD CIO is currently assessing which DoD policies will be impacted by the JIE's planning, implementation, operation, and defense. In addition to understanding how policies need to be changed, this review is prioritizing review of these policies based on their criticality to JIE and their age. From an operational perspective, *implementing the JIE also will require significant changes to current IT operational doctrine, processes, and TTPs*. As the lead for the JOSG, USCYBERCOM – with the full participation of the DoD Components – is leading the development of a new operating doctrine. This new approach to IT operational doctrine will incorporates JIE concepts and be

consistent with evolving cyber-operations command and control doctrine and concepts.

Finally, it is important to note that in addition to impacting policy at the Department level, the JIE also will impact policies within the DoD Components. As such, the Department is developing and revising a body of DoD-level directives, instructions, and manuals that comprehensively and consistently instruct the DoD Components on how to perform their statutory and regulatory responsibilities. These policies also must be sufficiently detailed, so the Components do not feel a need to develop and issue additional levels of supplemental policies. Risks associated with these Component-level supplemental policies could include misinterpretation of the original intent behind the DoD policy.

A(5) Capability Gaps and Dependencies

Introduction

Capability gaps and dependencies are relevant to the JIE effort. Many Joint Capabilities Integration and Development System (JCIDS) documents describe the gaps and capability achievement requirements that the JIE strives to address. These include:

- Joint Cyber Situational Awareness Initial Capabilities Documents (ICD)
- Cyber Attack ICD
- Mission Need Statement for Computer Network Defense
- Computer Network Attack ICD
- Future Mission Network ICD
- Global Information Grid (GIG) 2.0 ICD
- Global Information Assurance ICD
- Cross Domain Enterprise ICD
- Multinational Information Sharing ICD

In depth discussions concerning operational gaps and dependencies remain classified.

Dependencies

The *DoD Components are engaged in a number of critical activities on which the JIE depends*, including laying the foundation for the JIE through consolidating data centers, as part of the Federal Data Center Consolidation Initiative (FDCCI); consolidating DoD Component networks; normalizing software applications; and increasing DoD's purchasing power through the use of enterprise contracting initiatives. *Some specific examples of these dependencies include*:

- ***Data Center Consolidation*:** DoD will continue to consolidate computing power by closing and consolidating data centers across the Department as part of FDCCI. The Department also will identify existing data centers to be transitioned into a limited number of JIE CDCs.

Finally, DoD will accelerate efforts to normalize, rationalize, and reduce the number of the functional software applications that it has in use; this will drive out the duplicative and unnecessary applications that increase licensing and support costs. Adoption of cloud computing technologies must be incentivized and facilitated in smart ways that enable more effective and efficient sharing of commodity IT functions and enhance warfighter agility, survivability, and lethality.

- ***Normalization and Consolidation*:** DoD will continue normalizing and consolidating its network infrastructure at the B/P/C/S or equivalent levels. 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. These efforts will be leveraged toward a DoD network normalization and federated end state. The Department also will broaden planning and implementation of network technologies, such as Multi-Protocol Label Switching (MPLS), that will enable DoD to enhance operational effectiveness and improve its network security posture.

- ***Enterprise Services*:** DoD will continue to accelerate the implementation of enterprise services, such as Enterprise Directory Services and Enterprise E-mail, and begin implementing complementary capabilities, such as Enterprise SharePoint and File Storage, that will provide the warfighter with increased capabilities at a lower cost. At the same time, the Department will continue to stress and direct the sunset of DoD Component legacy systems with their stove pipe services.

- ***Governance and Oversight*:** 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) and budget lines. Program Element (PE) accounting codes will be aligned to support the JIE. Enabling DoD 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 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(6) Personnel Challenges

Introduction

This section introduces future personnel-related challenges specific to implementing the JIE, with a focus on *both civilian and military personnel, cyber workforce development, and training and certification.* A more detailed examination of this challenge will be provided in the future as a separate report as prescribed in NDAA Section 931(b).

As background, as the DoD is developing and implementing the JIE, the Department will also be transitioning and transforming its workforce. This essential transformation will ensure that the DoD can structure, operate, and defend its information, networks, systems, services, and capabilities in order to achieve operational and strategic advantage. The Department needs highly skilled IT managers who can govern the JIE, as well as operational personnel who can communicate and coordinate across DoD Component command structures to conduct offensive, defensive, and sustainment missions. To achieve this goal, DoD must recruit and retain qualified individuals with the necessary competencies and skills, and provide them with requisite education, training, certification, and developmental opportunities.

Civilian Personnel

The DoD competes with both the public and private sector for skilled cyberspace personnel. Going forward, Department leadership will continue to focus on how to make the DoD an employer of choice for new and rising cyber and IT talent. While DoD offers unparalleled opportunities to gain … cyber/IT experience, issues such as salary levels will remain a challenge. In fact, IT salaries within the private sector were projected to increase over 5 percent in 2013.This projected growth contrasts sharply with multi-year, stagnant government wage rates; a mandated defense-wide 2013 pay cut due to sequestration; the continued erosion of the IT special salary rates applicable to the federal Computer Science, Computer Engineering and IT Management occupations; and shrinking resources to pay recruitment, retention or performance bonuses. While current staffing vacancies will facilitate IT efficiency-driven force reductions, continued management attention is required to sustain this key segment of the cyberspace workforce.

Military Personnel

The JIE requires the Military Departments to allocate and align personnel resources to better support Combatant Command and Military Service priorities. New workforce demands, such as the cyberspace operational forces required to staff USCYBERCOM, as well as individual Military Service requirements, must be met and may require force trade-offs. *Long-term personnel efficiencies are an anticipated result of the Department's drive to produce IT efficiencies*, which includes optimization of networks, standardization of hardware and software platforms, consolidation of data centers, and virtualization of applications. However, the net impact on IT and cyberspace staffing is still being assessed and will be defined in the forthcoming personnel plan required by the FY13 NDAA.

Cyber Workforce Development

Effective workforce management practices also will be integral to the success of the JIE. *The Department is currently finalizing an overarching policy for cyberspace workforce management*. This directive will instruct DoD Components to identify the billets needed to develop, operate, maintain, secure, defend, and fight within JIE by using a common set of standards. It also will require that each Component identify members of its cyberspace workforce, then ensure that these personnel are qualified in accordance with a Department-wide standard. This benchmark will be based on the functions they perform, and the Component will evaluate the individual prior to assigning them to a cyberspace billet.

To allow for easy identification of like skill sets across the Components and with other federal agencies, industry, and post-secondary educational institutions, *the Department must develop a set of workforce standards that align with the National Initiative for Cybersecurity Education (NICE), Cybersecurity Workforce Framework*. This DoD Cyberspace Workforce Framework will enable:

- Improved joint operations
- Efficient translation of roles across personnel occupations
- Standard position descriptions
- Unified core competencies
- Across-the-board training and education
- Practical exercises
- Rapid surge support, when required

Training and Certification

In addition to aligning and organizing the workforce to operate within the JIE, the DoD is establishing common training standards and ensuring the availability of requisite classroom, online, and on-range activities training for military and civilian personnel. To date, Component cyberspace training has been conducted mostly by the Military Services, including the Joint training efforts of CYBERCOM through the Joint schoolhouses operated by the NSA, the Air Force Institute of Technology, the Naval Post Graduate School, and at the National Defense University (NDU).

The Department is working to increase the availability and regularity of Joint training to optimize operations in the JIE and has established the Cyberspace Training Advisory Council (CYTAC) to synchronize training and readiness standards. DoD also is increasing the use of cyber ranges at the Component level as well as Joint exercises to enhance individuals' ability to operate in a Joint environment. Increasing training and readiness standards across the Department will enable the DoD to change how it operates and fully take advantage of the efficiencies gained from the transition to the JIE.

B. Conclusion

The current DoD IT environment is dominated by independently developed, acquired, and managed Component- and installation-specific capabilities. It is a complex layering of multiple networks with overlapping, duplicative roles and responsibilities, and as stated by the Commander of CYBERCOM, the current network is "not defendable."

For this reason, the DoD must move to an environment that will enable *the Department's vision and strategy for United States military forces as they execute their assigned missions in all operational environments*. Recognizing that today's mission success depends upon the ability of military commanders, civilian leaders, and mission partners to act quickly and effectively, based on the most accurate and timely information available, DoD has undertaken an unparalleled realignment and restructuring effort that addresses how its IT networks, systems, and services are constructed, operated, and defended.

Achieving the JIE will improve mission effectiveness by assuring access to information on any device, at any time, under all conditions, whenever the warfighter needs it. It also is designed to increase cybersecurity, strengthen business operations, and reduce long-term IT infrastructure costs. This complex, long-term, transformational effort will require the continued guidance and oversight of DoD leadership. Their full engagement is critical as implementation opportunities and challenges to achieving the JIE arise across the Department.

Finally, the DoD cannot achieve this transformation alone. Collaboration and dialogue with mission, industry, and academic partners, as well as with the support of Congress, will be central to identifying best practices and working through the myriad of technical challenges which must be overcome. As a Department and as a nation, we owe this level of effort and collaboration to the warfighters who depend on these technologies as they defend our nation at every level, every day.

This page intentionally left blank.

C. References

APPENDIX A – STATUTORY LANGUAGE

SEC. 931. Implementation Strategy for Joint Information Environment.

(a) Implementation Strategy. Not later than March 31, 2013, the Secretary of Defense shall submit to the congressional defense committees a strategy for implementing the Joint Information Environment. Such strategy shall include –

(1) A description for the vision for the Joint Information Environment, including a roadmap for achieving such vision from the existing baseline architecture;

(2) An assessment of the key milestones, metrics and resources needed to achieve such vision, including the anticipated implementation cost and lifecycle cost savings of the Joint Information Environment;

(3) A description of the acquisition strategy and management plan for implementing the Joint Information Environment;

(4) An analysis of the key technical and policy challenges that must be addressed to achieve such vision, including assignment of responsibility for addressing such challenges.

(5) An identification of dependencies with existing initiatives or programs and capability gaps not currently addressed by funded initiatives or programs; and

(6) An assessment of the personnel challenges associated with manning, training, operating, defending, and fighting in the Joint Information Environment as a command and control and weapon system.

(b) PERSONNEL PLAN. Not later than one year after the date of the enactment of this Act, the Secretary of Defense, in consultation with the Chairman of the Joint Chiefs of Staff, shall submit to the congressional defense committees a Department-wide personnel plan for making the Joint Information Environment operational. Such personnel plan shall be based on the strategy required under subsection (a) and shall include a validated Joint Staff requirement for manpower levels and the levels required for each of the military departments and combat support agencies needed for full spectrum cyber operations, including the national cyber defense mission and the operational plans for the combatant commands, for each fiscal year across the current future-years defense program.

This page intentionally left blank.

APPENDIX B – 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
DISR	Department of Defense Information Technology Standards and Profile Registry
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
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
IAW	In Accordance With
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

This page intentionally left blank.

APPENDIX C – LIST OF TABLES

This page intentionally left blank.