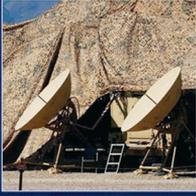


Joint Net-Centric Operations Campaign Plan

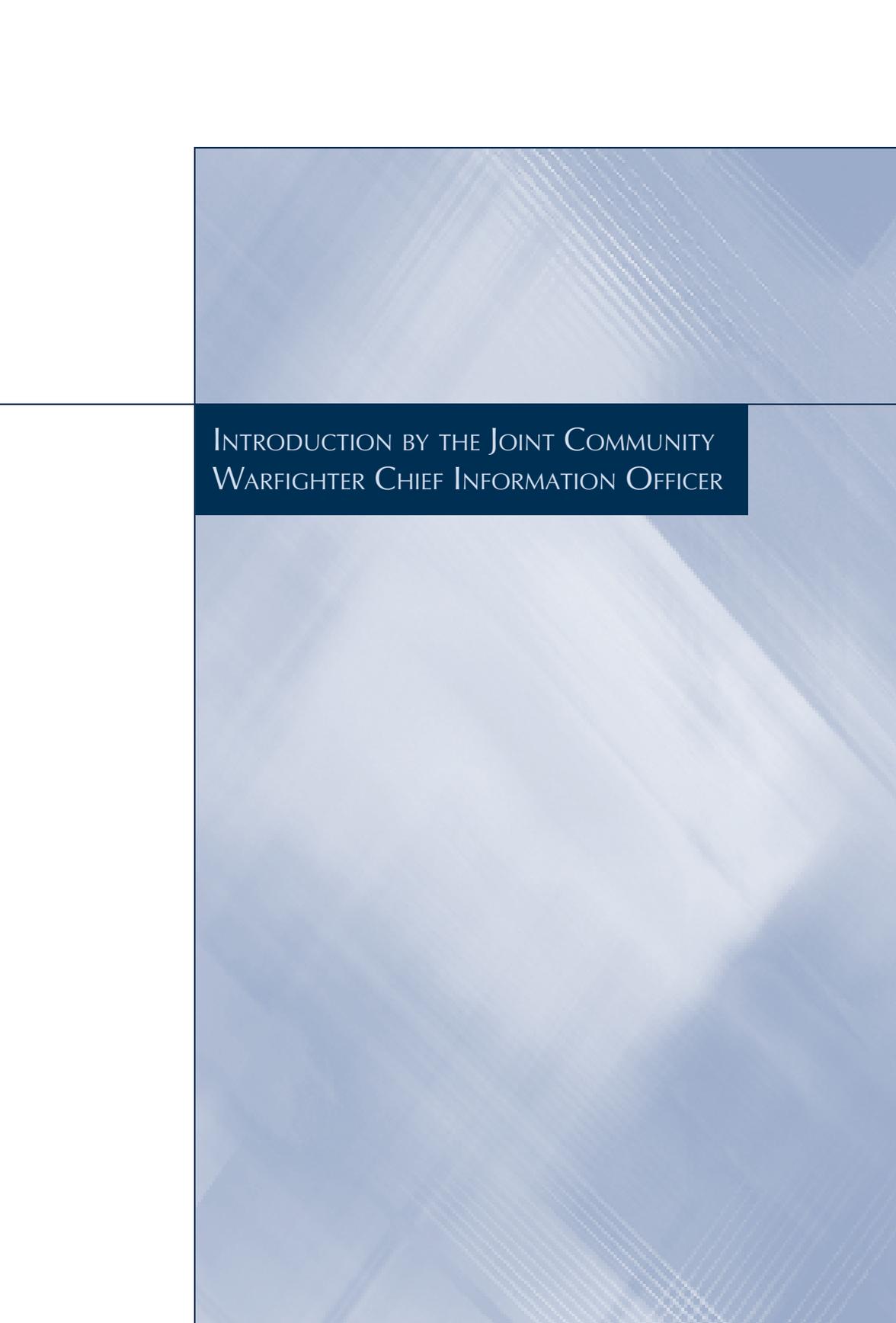


Joint Staff

*Command, Control, Communications
and Computer Systems Directorate (J-6)*



October 2006

The background of the page features a complex, abstract pattern of overlapping, semi-transparent blue lines and shapes, creating a sense of depth and movement. A dark blue horizontal band is positioned across the middle of the page, containing the text. The text is in a white, serif font, centered within the band.

INTRODUCTION BY THE JOINT COMMUNITY
WARFIGHTER CHIEF INFORMATION OFFICER

Nancy E Brown
VADM Nancy Brown

Director, C4 Systems
The Joint Staff

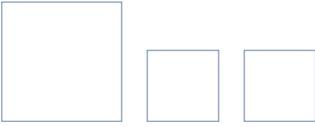


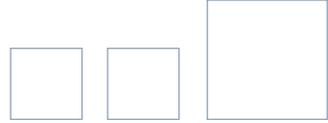
The Joint Community has been extremely busy since LtGen Shea published the first Joint Command, Control, Communications and Computer (C4) Systems Campaign Plan in September 2004. I am pleased to say that cooperatively we have improved capabilities to the joint force through progress in completion of the action items in the previous plan. However, we still have a long road in front of us.

Despite the passage of time, some things remain constant. The Global War on Terrorism continues to be our top priority, as does our need to accelerate transformation throughout the joint force. We have made great headway in improving our net-centric capabilities, but many of our toughest challenges remain ahead.

Ultimately, our vision is full implementation of the capabilities that Joint Net-Centric Operations makes possible for the joint force. To continue on this journey, my staff organized the campaign plan around a strategy which focuses our efforts, over the next 2 to 5 years, on broad goals, specific objectives and achievable actions. Our success will continue to improve the joint net-centric capabilities we deliver to the warfighters—moving from unsynchronized to more interoperable and ultimately, to fully interdependent capabilities. Full realization of the capabilities that a net-centric operations environment provides requires a culture that knows how to use and take advantage of it. This will take a fundamental shift in processes, policy and culture. It will take all of us working together to identify the barriers and remove them. I am confident we will be successful and look forward to the journey.

This document is the first update since 2004. We have made a concerted effort to include your thoughts, inputs and feedback. We do not profess to have all the answers and look forward to your inputs and comments as we continue to integrate our efforts to realize the joint net-centric vision.





1 Background

- Purpose
- Scope
- Organization
- Assumptions
- The Environment
- Strategic Guidance
- Challenges

9 Strategy

- Strategic Concept
- Goals and Objectives

27 Way Ahead

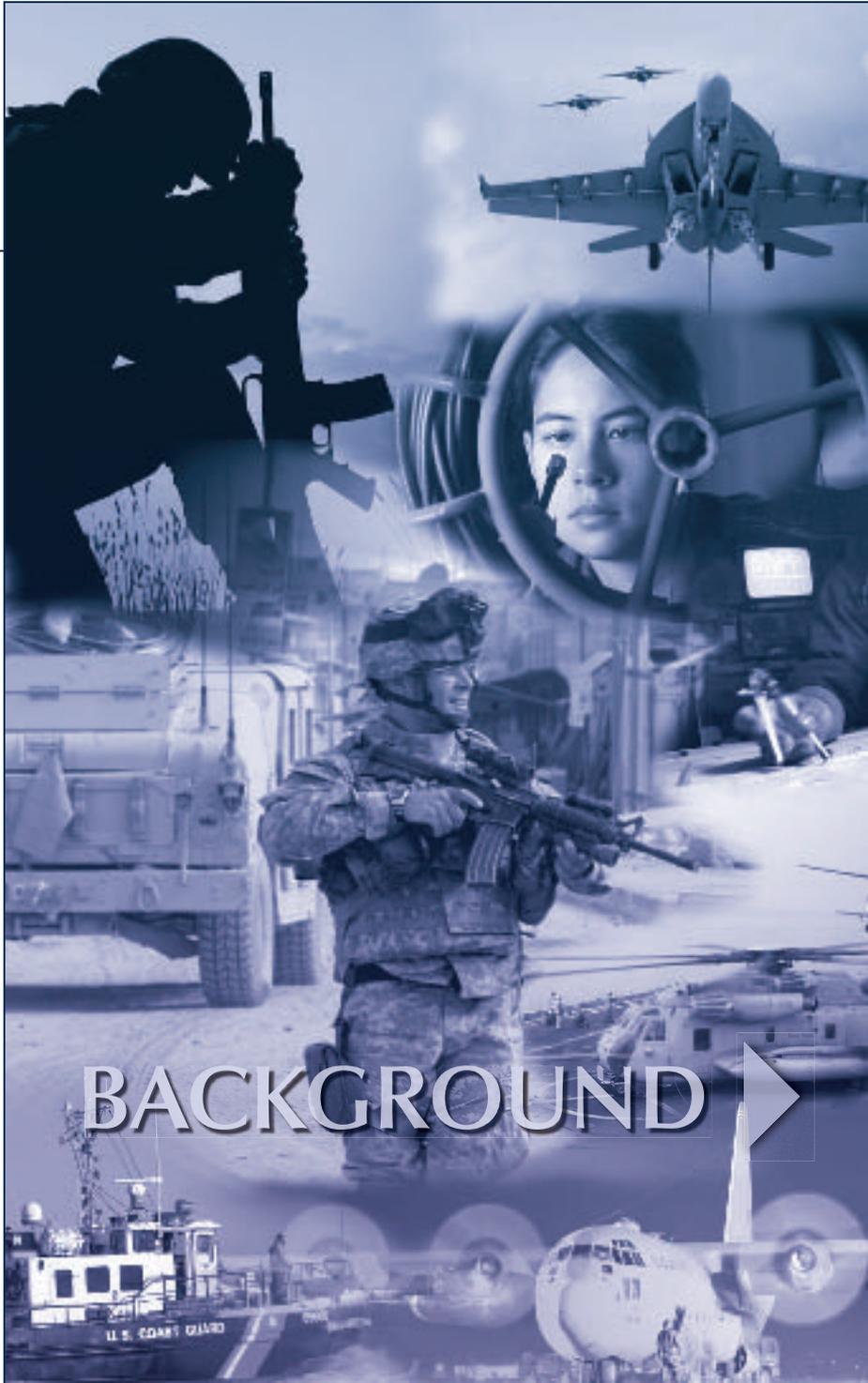
29 Annex A – Goals, Objectives and Actions

43 Annex B – System, Service and Organization Descriptions

51 Annex C – Established Processes

55 Annex D – Glossary: Acronyms and Definitions

67 Annex E – References



BACKGROUND



Purpose

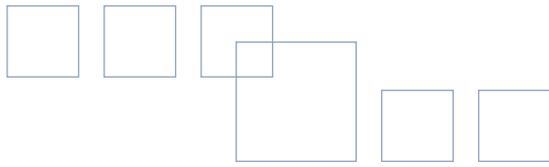
This plan is published by the Joint Community Warfighter (JCW) Chief Information Officer (CIO) (Director, Joint Staff/J-6) to provide a unifying strategy to better integrate and synchronize joint community transformation and maximize joint warfighting capabilities.

In September 2004, the JCW CIO published the first *Joint C4 Campaign Plan* to contribute to Department of Defense (DOD) transformational efforts and to meet the challenges posed by the Global War on Terrorism (GWOT). The intent was for the *Joint C4 Campaign Plan* to serve as a living document to be progressively updated. Much has happened since September 2004, both in the joint community and throughout the Department of Defense in general.

First, there is new strategic guidance, including the *National Security Strategy—March 2006*, *2006 Quadrennial Defense Review (QDR) Report*, the *2006 Strategic Planning Guidance (SPG)* and the *16th Chairman's Guidance to the Joint Staff*. These documents detail the strategic direction of the Department and the net-centric capabilities to be employed by the joint force.

Second, there has been significant progress in the development of net-centric concepts. Both the *Joint Net-Centric Environment (NCE) Joint Functional Concept* and *Net-Centric Operational Environment (NCOE) Joint Integrating Concept (JIC)* were approved by the Joint Requirements Oversight Council (JROC), providing a description of the operational-level net-centric capabilities required to support contingencies across the continuum of military operations, key attributes necessary to compare capability solution alternatives and how future joint force commanders (JFCs) will employ net-centric capabilities.

The NCOE program is evolving into Joint Net-Centric Operations (JNO). The next version of the *NCE Joint Functional Concept* will be titled the "*JNO Joint Functional Concept*" to reflect the ongoing work to refine capabilities in the net-centric area. During transition "JNO" is the applicable term, but both may still be used



depending on timeframe and context. There are scope and technical differences in NCOE, NCE and JNO. However, in order to simplify this document for the reader NCOE, NCE and JNO capabilities will be collectively referred to under the term “JNO.”

Scope

This plan is intended to be used cooperatively by members of the joint community to establish and prioritize recommendations for implementing improvements in doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF). The focus of this document is on activities that must occur in the next 2 to 5 years to make substantive progress toward the full range of JNO capabilities outlined in transformational capabilities and concept documents. The joint community “vision” or long-range target set of capabilities is embodied in the JNO. The “vision” is full implementation of the capabilities the JNO makes possible for the joint force—an integrated global network that enables us to share the right information at the right time so you can act before the enemy acts. End-state goals in this plan may not be fully realized for 10 or more years. However, it is clear that coordinated activity must occur now to reach the goals and achieve the full benefits of a networked force. It is envisioned that operational planners will use this plan as a reference in the development of joint warfighting concepts, plans, doctrine and tactics, techniques and procedures (TTPs).

Organization

This plan is organized into three sections and five supporting annexes:

- **BACKGROUND** – Discusses assumptions, the current operating environment of our forces, guidance from strategic documents and near-term challenges faced by the joint warfighter.
- **STRATEGY** – Presents a coordinated joint community strategy to achieve stated goals and progress toward the full range of JNO capabilities.
- **WAY AHEAD** – Summarizes the way forward by establishing this plan as a living document.
- **ANNEXES** – Presents details of the strategy and other supporting information. In order to keep this a living document, Annex A (Goals, Objectives and Actions) which contains the details of this plan’s actions, is located on the Internet at <http://www.jcs.mil/j6/jointcampaign.html>.

Assumptions

The United States will remain engaged in a war against terrorism over the plan’s life. The US Armed Forces will continue to work in cooperation with many non-DOD partners, such as North Atlantic Treaty Organization (NATO) allies, coalition partners established for a specific conflict, federal agencies, non-governmental organizations and the commercial sector. Our adversaries, the environment, operational concepts and technological capabilities in use today will continue to evolve at a rapid pace.



Transformational capabilities and future warfighting concepts will continue to evolve to meet these challenges for the foreseeable future.

The Environment

As the Department of Defense enters the fifth year of the GWOT, a war termed the “long war,” the US Armed Forces continue the ongoing process of transformation. We are in an era characterized by uncertainty and surprise. Our adversaries will continue to focus on the use of asymmetric capabilities that avoid US strengths and exploit potential vulnerabilities. Current and future adversaries will adapt as our capabilities evolve. The world, including our adversaries,

is empowered through interconnected networks and technology supplied by the global industrial base. Increased availability of digital communications, encryption techniques, global positioning and the Internet give our adversaries new capabilities and the potential ability to disrupt our information systems at a relatively low cost. We are fighting a war in the information domain and the enemy is out maneuvering us.

After the terrorist attacks of September 11, 2001, the Department of Defense accelerated its transformation process. As a result, today’s joint force is more expeditionary, modular and agile. Technical advances, including improvements in information management and precision

The Strategic Environment	
Past	→ Present
Peacetime tempo	→ Wartime sense of urgency
Reasonable predictability	→ Era of surprise and uncertainty
Single-focused threats	→ Multiple, complex challenges
Nation-state threats	→ Decentralized network threats from non-state enemies
War against nations	→ War in countries we are not at war with (safe havens)
“One size fits all” deterrence	→ Tailored deterrence for rogue powers, terrorist networks, and near-term competitors
Crisis response (reactive)	→ Preventive actions – shaping the future (proactive)
Threat-based planning	→ Capabilities based planning
Peacetime planning	→ Rapid adaptive planning
Focus on kinetics	→ Focus on effects
20th century processes	→ 21st century integrated approaches
Static defense, garrison forces	→ Mobile, expeditionary operations
Under-resourced, standby forces (hollow units)	→ Fully-equipped and fully-manned forces (combat ready units)
Battle-ready force (peace)	→ Battle-hardened forces (war)



weaponry, allow the joint force to generate considerably more combat capability with the same or fewer weapons and at lower manning levels. In the midst of a continuing GWOT, the US military force posture has emphasized the ability to surge quickly to trouble spots across the globe. In the 2006 QDR Report, senior DOD leaders characterized the progress of DOD transformation through examples of changes that have occurred to better meet the new strategic environment.

Strategic Guidance

Sources of strategic guidance used in the development of this plan are shown below. In addition to these documents, the Campaign Plan is influenced by the Chairman’s Priorities on the next page.

Strategic Guidance

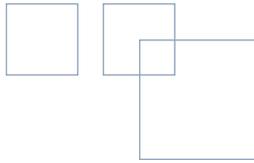
- National Security Strategy
- National Defense Strategy
- National Military Strategy
- Quadrennial Defense Review Report
- Transformation Planning Guidance
- Strategic Planning Guidance
- Joint Operations Concepts Family

Challenges

Significant progress has been made in improving net-centric operations capabilities. Progress includes establishment of governance responsibilities; development of concepts, policies and guidance; and

implementation of several major programs and initiatives that lay the infrastructure foundation for network operations (NetOps). However, numerous challenges still face the joint community as we build upon accomplishments made to date in transforming from platform and organization-centric to a net-centric force. The following major challenges are addressed by the goals and objectives presented later in the “Strategy” section and in more detail in Annex A:

- Insufficient Assured Warfighter Connectivity. Combatant commanders’ rapidly evolving joint operational needs are not being completely met. Principally, there is insufficient connectivity and bandwidth for warfighters operating at the “first tactical mile.” Increasing satellite communications (SATCOM) requirements, reliance on aging military SATCOM constellations and delays in fielding new systems contribute to the gap between operational requirements and fielded capabilities. Additionally, operational requirements point to the need for more capable wireless technologies, as well as a commitment by the joint community to resolve interoperability and integration issues affecting the joint force. Global Information Grid (GIG) implementation guidance continues to mature; however, enforcement mechanisms are not yet in place. Finally, how the Department will transition from Internet Protocol (IP) version 4 to IP version 6 (IPv6) and what impact this transition will have on joint operations and capabilities still needs to be determined.

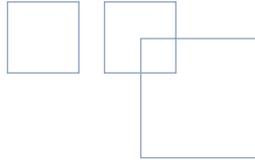


Chairman's Priorities

- (1) Win the Global War on Terrorism
 - Information, perception and how and what we communicate are critical
 - Assist others to create an environment in which terrorism will not flourish
 - Integrate and coordinate our efforts within the Department of Defense and the interagency
- (2) Accelerate Transformation
 - Transformation is a continual process, not an end state
 - Transformation is as much a mindset and a culture as it is a technology platform
 - Transformation is a willingness to embrace innovation and accept analyzed risk
- (3) Strengthen Joint Warfighting
 - Produce a force capable of swiftly and decisively defeating any enemy
 - Focus on transitioning from an interoperable to an interdependent force
 - Individual Service perspectives brought together jointly foster better solutions
- (4) Improve the Quality of Life (QOL) of Our Service Members and Their Families
 - Bring our people home alive and intact is QOL Job #1
 - Applies to the total force—Active, Guard and Reserve, military and civilian
 - Preserve the ethos of the warrior
 - Pace yourself and your subordinates: it is a marathon, not a sprint

■ Lack of an Integrated and Synchronized Approach to Common Enterprise Services Development and Delivery. The Defense Information Systems Agency (DISA) and the Services are developing common enterprise services (ES) to support operations at every level including the tactical user. Despite ongoing efforts to converge on agreed standards, there is no single set of technical guidelines for common ES. In part, this is because

best practices and standards are being developed in parallel with the common ES themselves; this same situation (parallel development of standards and services) is occurring in industry as well. Possible risks associated with parallel development include a lack of interoperability, redundant efforts and failure to take advantage of “economies of scale,” all of which could impact services at every level.



■ **Lack of Adequate Protection Against Increasing Threats to DOD Networks and Information.** DOD networks are under constant attack. The gap between identifying a network vulnerability to the time of adversary exploitation has narrowed. Protection of networks and information during transmission, processing and storage must be improved to assure operational availability of information and networks at all times, including while under attack.

■ **Inadequate Ability to Share Operational Information with Mission Partners.** The need to share information has been identified by seven of the nine combatant commands in their Integrated Priority Lists (IPLs). The Department of Defense lacks an information sharing strategy to guide the transition from today's information sharing paradigm to a net-centric paradigm. Information sharing today occurs via interconnected physical networks separated by classification, whereas information sharing in a net-centric paradigm

needs to be based upon individual mission requirements and role-based access. Data strategy efforts enabling communities of interest (COI), cross-domain solutions (CDSs) and knowledge management (KM) capabilities enabling secure information sharing with Joint, multinational, interagency, state, local and first responder mission partners are inadequate to mission needs.

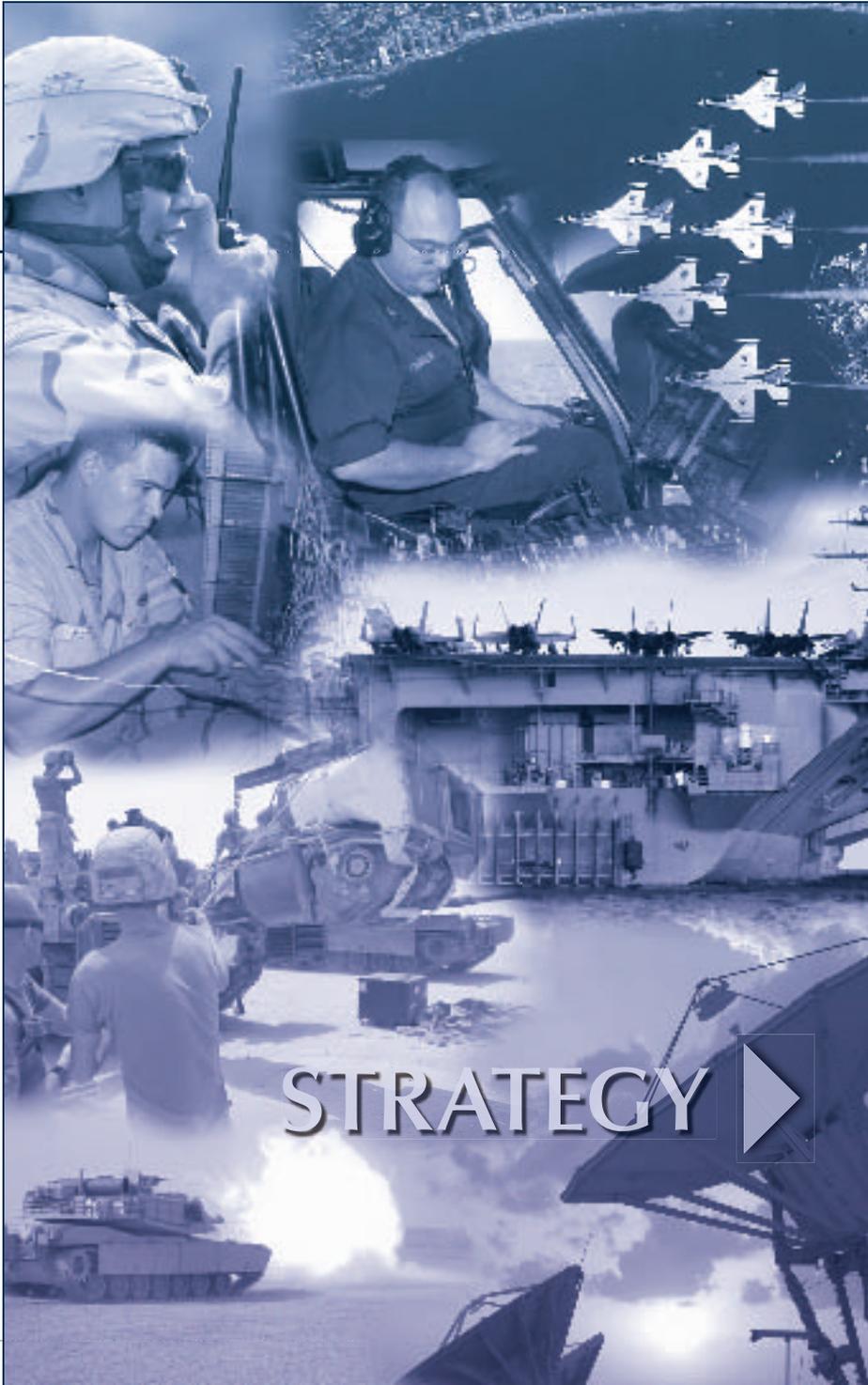
■ **Lack of a Fully Integrated Approach to the Delivery of Joint Networking Capabilities.** Historically there has been a disjointed approach to identifying, acquiring, testing, evaluating, integrating and fielding joint communications capabilities. This disjointed approach creates complex challenges in the areas of capability specification, configuration management, program synchronization, performance tradeoff analysis and the ability to quickly take advantage of emerging technology. This situation wastes resources and limits DOD ability to deliver coordinated solutions that allow fully interoperable joint and multinational operations.





- Lack of a Mature GIG Enterprise Management Capability. The ability of the GIG to rapidly adjust to meet changing warfighter needs and translate mission needs into balanced network taskings is lacking. NetOps is the integration of GIG Enterprise Management (GEM), GIG Network Defense (GND) and Information Dissemination Management (IDM)/Content Staging (CS) capabilities to operate and defend the GIG. We are continuing to “operationalize” the network (i.e., treating it with the same rigor and discipline that is applied to weapons systems and those who control and operate them). NetOps is maturing, but continues to be hampered by ambiguous command relationships, insufficient end-to-end situational awareness and incomplete GIG operations and defense policy and implementation directives.





STRATEGY

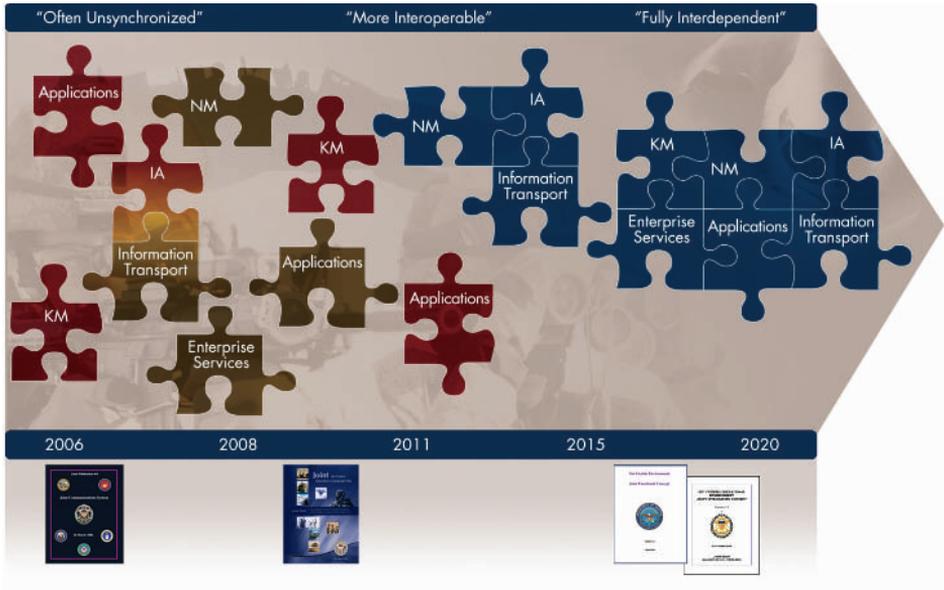
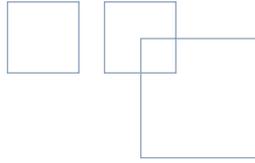


The JNO Strategy consists of a strategic concept, goals, objectives and actions to be accomplished over the next 2 to 5 years to make substantive progress toward the full range of net-centric capabilities currently outlined in transformational capabilities and concepts documents. Illustrated on the following page is the timeframe focus of joint doctrine, this campaign plan and net-centric future concepts. It also shows that as we move from today to 2015-2020, net-centric capabilities will transition from often unsynchronized to fully interdependent.

This section outlines the strategic concept, goals and objectives. The strategic concept sets the overarching direction for the JNO effort. The goals are purposely broad with the objectives and actions focused primarily on the 2 to 5 year timeframe. The list of actions that will enable us to achieve the broader objectives and goals are outlined in Annex A. Actions will be refined as progress is made within objectives. The strategy originates primarily from two transformational concept documents: the *NCE Joint Functional Concept* and the *NCOE JIC*, which were vetted through the joint concept development process.

Net-centric capabilities fall within the JNO Joint Capability Area (JCA), one of the 21 Tier 1 JCAs endorsed by the Secretary of Defense. A Tier 1 JCA is a high-level capability category that facilitates capabilities-based planning, major trade analysis and decision-making. JCAs provide a common capabilities language for use across many related DOD activities and processes. The JCA structure will eventually be extended down to the task level to replace the current Universal Joint Task List.

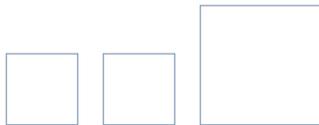
There is a concerted effort to coordinate the strategic plan of the DOD CIO (the Assistant Secretary of Defense (Networks and Information Integration) (ASD(NII))) and the Joint Community CIO's JNO Campaign Plan. The JNO Campaign Plan is outlined in the remainder of this section, beginning with the strategic concept.



Joint Net-Centric Operations Strategy

Strategic Concept

- JNO is a future framework that connects the human and technical power of the joint force and its mission partners to share needed information at the right time and format, while protecting it from those who should not have it.
- By incorporating the capabilities needed to respond to the dynamic needs of warfighters through KM, the NCE provides more than a networked set of technical capabilities. JNO can be thought of as a vastly improved synergy of DOTMLPF and policy, energized by the advances of the information age—a synergy that will enable warfighters and other decision makers, at every level, to make and execute superior decisions faster than adversaries.
- The JNO has six operating capabilities. The seamless integration of these capabilities will assist the JFC across the range of military operations:
 - KM
 - Information Assurance (IA)
 - Network Management (NM)
 - Information Transport
 - ES
 - Applications
- **JNO Operational Context.** The JNO's operational context is "built" upon a globally accessible platform of data and information. Access to information is provided through information transport mechanisms that enable the processing of that data and information via ES, interfaced to the users via the JNO's applications. KM, NM and IA

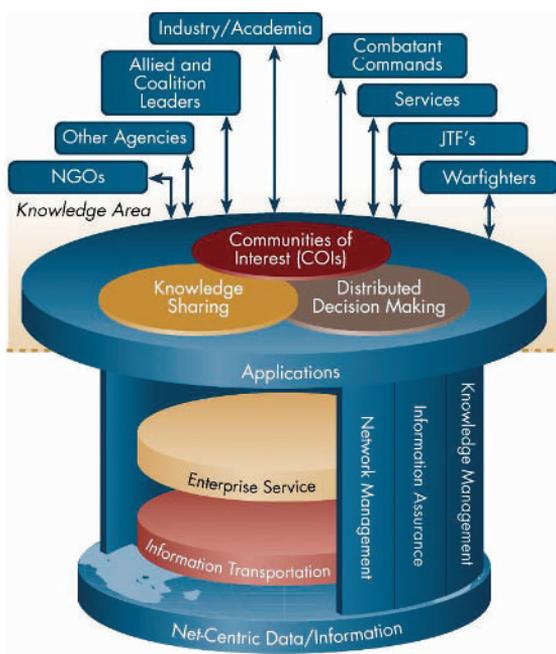


functions integrate the JNO, providing the warfighter or user with a seamless capability to collect, create and use actionable knowledge in an operational context. Given that the JNO operational context is built upon data and information, its success hinges on implementation of the DOD Data Strategy and COIs.

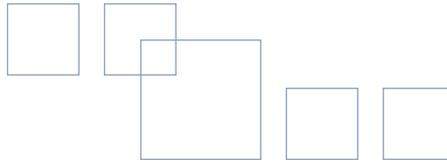
■ **Pervasive Knowledge**

- JNO leverages non-material advantages such as human knowledge as much as technical network advances; dramatically improves how major combat operations can be planned and conducted; and dynamically supports operations at every echelon, especially warfighters at the “first tactical mile.”
- Pervasive knowledge, the outcome of knowledge sharing generated through the JNO, will produce many warfighting advantages. The Major Combat Operations (MCO) Joint Operating Concept (JOC) states, “Our pervasive knowledge capability forms the core of all other capabilities, for it provides the knowledge base from which decisions are made and actions taken. Our ability to see and understand first enables us to decide and act first.”
- The Observe, Orient, Decide, Act (OODA) Loop is a well-known construct for military decision-making.

In the past and to a large extent today, the individual warfighter at the “first tactical mile” lacks access to timely, secure and actionable information at all phases of the OODA Loop. Legacy communications and stovepipe network capabilities were primarily enablers of the “Orient” phase, providing warfighters with situational awareness. Individuals working within military functional lanes (e.g., personnel, intelligence, operations and logistics) contribute information to support other phases of the OODA Loop, but stovepipe networks and incomplete data formats prevent information from being directly accessible by individual warfighters.



The JNO Operational Context



JNO-OODA Loop Integration

□ In contrast, the JNO capability area is integrated into all four phases of the OODA Loop. Through the JNO, warfighters will access secure information from both inside and outside their immediate environment and will *observe* real-time events and receive feedback from previous actions. Through networking and synthesizing data from traditionally separate staff functions and collaborating with mission partners, warfighters will *orient* on the unfolding situation, as the network responds to their changing operational needs. Due to the warfighter's access to relevant information and knowledge, including the latest intelligence, surveillance and reconnaissance (ISR) reports, the current operational picture and insights of subject matter experts and/or COIs, the warfighter will *decide* on appropriate courses of action and will *act* with improved effectiveness and enable a new range

of warfighting capabilities. Through repetition of this collaborative process throughout the battlespace, networked warfighters' knowledge is developed and shared, thereby increasing the pervasive knowledge capability of the overall joint force.

- **Benefit to the Warfighter.** In addition to the warfighting advantages that result from pervasive knowledge, the JNO supports a broad range of military functional areas—specifically, the ability to share relevant information rapidly and securely. The JNO contributes to joint warfighting by:
 - Reducing warfighters' decision cycle and enabling superior decision making.
 - Supporting the creation of a trained and ready pool of joint task force (JTF)—capable headquarters, ensuring a wider range of military response options.



- Enhancing Homeland Defense efforts, including the ability to detect threats in the approaches and interdict them at a distance as well as providing military assistance to civil authorities in support of natural disasters.
- Improving human intelligence, ISR, airborne surveillance and airlift capacity and specialized naval forces configured for coastal and riverine operations.
- Enabling foreign training and security missions via special operations forces and traditional ground forces, strategic communications efforts to effectively convey the DOD message and coordination within the Department and with our international partners to maximize military power.

■ **Goals.** The six JNO operating capabilities serve as a framework for the JCW CIO goals. The goals and their accompanying objectives are discussed in detail in the following paragraphs:

- **Goal 1** – Connect the Warfighter
- **Goal 2** – Leverage the Power of Enterprise Services
- **Goal 3** – Secure the Network
- **Goal 4** – Accelerate Information Sharing
- **Goal 5** – Synchronize Delivery of Network Capabilities
- **Goal 6** – Transform GIG Enterprise Management and Enhance Electromagnetic Spectrum Access

Goals and Objectives

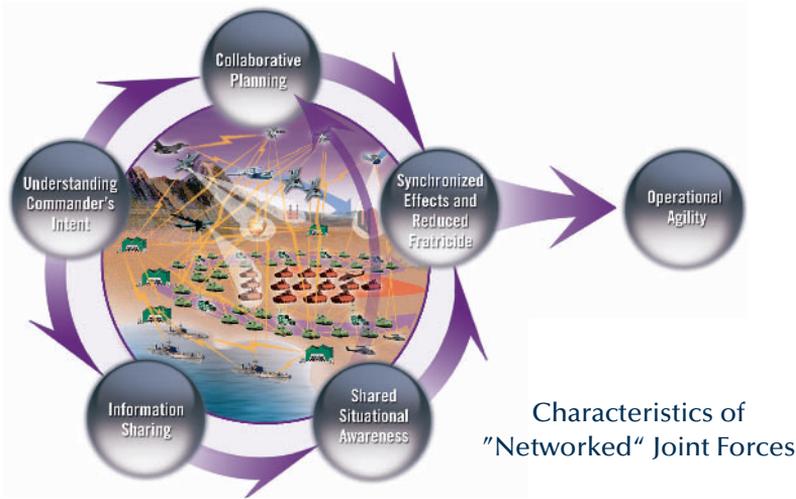
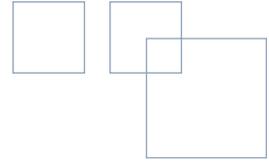
Goal 1 – Connect the Warfighter

1

It is essential that seamless communications services be available to joint warfighters and mission partners under all conditions and at every echelon—especially at the “first tactical mile.”

Connecting the warfighter is essential to the Chairman’s goal of “Strengthening Joint Warfighting.” The JNO is the key to providing transformational communications capabilities to the warfighter. Information transport provides the foundation for the JNO by combining assured, timely, resilient and survivable connectivity with dynamic network management capabilities to the “first tactical mile” users. Wireless capabilities and effective network integration are also necessary to assure communications in a highly dynamic joint warfighting environment. By delivering effective network connectivity and interfaces, the joint force





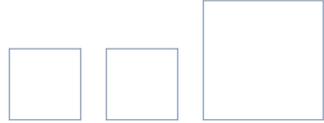
will be able to effectively tap into key information transport capabilities that enable information sharing at all levels—from the “first tactical mile” to the national level.

Goal 1 Intent:

The joint community must partner with relevant organizations to develop a DOD strategy to satisfy warfighter’s beyond line-of-sight communications needs. The strategy should assess emerging technologies such

as tactical satellites, near-space platforms and unmanned systems to increase transport capabilities and alleviate demands on oversubscribed SATCOM systems; it should also include recommendations on striking a balance between military and commercial SATCOM and alternatives to space-based capabilities. The strategy must also address how programs continue to remain synchronized and on schedule throughout requirements definition and cost control efforts. US Strategic Command (USSTRATCOM) conducts regularly scheduled SATCOM exercises (e.g., wargaming) and other SATCOM assessments to determine the correct capability mixture of commercial and military satellite assets, including ground segment resources. A periodic review and re-validation of all satellite requirements is required to ensure the accuracy of the SATCOM database and facilitate USSTRATCOM’s assessments.





The transition of the Defense Information System Network (DISN) to the next infrastructure requires the documentation of key processes. The joint community must oversee the collection, validation and implementation of joint warfighting capabilities into the existing information infrastructure and DISN. Transition to converged networks (i.e., convergence of DISN-Managed IP networks, including: Non-secure Internet Protocol Router Network (NIPRNET), SECRET Internet Protocol Router Network (SIPRNET) and others) and network services will be based on proven technologies and security that deliver required capabilities. The requirement for non-IP based redundant systems must be determined; reliance on converged communications must not expose the Department of Defense to an unknown or unacceptable level of risk.

Joint wireless capabilities provide tactical units net-centric connectivity to the GIG. A joint wireless concept of operations (CONOPS) is needed to articulate the DOD concept for wireless capabilities and to support JNO.

Lessons learned from exercises and real world operations provide critical feedback on system interoperability. The joint community must establish a collaborative process to categorize shortfalls, identify potential solutions and resolve issues.

To enable JNO, we must develop, maintain and enforce compliance with GIG implementation guidance. Two important guidance initiatives are represented by the development of key interface profiles (KIPs)

and net-centric implementation directives (NCIDs).

The joint community must actively support combatant commanders in meeting their rapidly evolving joint operational needs. The joint community must become familiar with the full range of joint processes and fora that best address issues and actively assist the combatant commanders in finding and using the most appropriate venue for solving issues.

The transition to IPv6 will be a gradual, market-driven process dictated by industry's distribution of IPv6 standards, equipment and services. The joint community requires a strategy and the means to validate performance of essential network services during DOD migration to IPv6.



Goal 1 Objectives:

- 1.1 Develop strategies for warfighter's beyond line-of-sight needs to include a balance between military and commercial SATCOM and alternatives to space-based capabilities.
- 1.2 Orchestrate collection, validation and implementation of joint warfighting capabilities into existing information infrastructure and DISN.



- 1.3 Develop joint wireless capability to support JNO.
- 1.4 Resolve interoperability and integration issues occurring within the operational environment.
- 1.5 Develop and enforce compliance of GIG implementation guidance to enable JNO, integration and data sharing in connecting to the GIG enterprise.
- 1.6 Maximize support to combatant commanders through joint programs, processes and venues to meet rapidly evolving JNO operational needs.
- 1.7 Develop a strategy and validate performance testing with delivery of essential network services throughout DOD migration to IPv6.



with minimal latency, to support the mission. The combatant commands, Services, agencies, Joint Staff and the Intelligence Community (IC) must work together to continually evolve operational requirements to achieve an enterprise-level foundation for NetOps. Participation in DOD efforts to strengthen its data strategies will be necessary for all partners. Additionally, the development of an information sharing strategy with multinational, state, local and non-government agency mission partners is necessary.

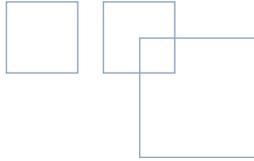
Goal 2 – Leverage the Power of Enterprise Services

Provide the warfighter with common enterprise solutions to improve information sharing and combat effectiveness.

Goal 2 Intent:

The Net-Centric Enterprise Services (NCES) program will develop strategies, facilitate the delivery of enabling policy and provide joint policy in support of DOD efforts to transition to ES. NCES provides common “enterprise-wide” services, adopting commercial and Service enterprise services as NCES enterprise solutions where possible. Core service functionality being developed includes: discovery, mediation, messaging, collaboration, security and NM. Multiple programs, initiatives and efforts across the Department are developing ES that have varying levels of applicability to the overall

The Department of Defense is developing common ES to facilitate information access and sharing. ES will allow dynamic, agile collaboration and accelerated decision cycles amid unprecedented quantities of operational data. The ES suite of capabilities with selectable attributes will support users in all operational environments and empower edge users to pull information from any available source,



DOD enterprise. An ES architecture is needed to detail where ES will be distributed and how they will be delivered from strategic and operational down to tactical users.

The joint community must develop policy, procedures and solutions to ensure ES capabilities are sufficient and available to meet the rapid deployment and employment of a JTF. The community must continue to define functional, organizational and operational requirements for Deployable Joint C2 (DJC2) System during its development. This process must ensure Increment 1 is fielded with a capability that meets the actual requirements reflected in its CDD. All partners must continue to participate in the development of the CONOPS, CDD and capabilities production document (CPD) of DJC2 Increment 2.

Goal 2 Objectives:

- 2.1 Develop strategies, facilitate enabling policy and provide joint guidance in support of DOD efforts to transition to ES.
- 2.2 Establish and advocate NCES capabilities required to support JNO.
- 2.3 Facilitate the transition and integration of DOD C2 and shared situational awareness efforts into a net-centric enabled environment.
- 2.4 Develop policy, procedures and solutions to ensure ES capabilities are sufficient and available to meet the rapid deployment and employment of a JTF.

Goal 3 – Secure the Network

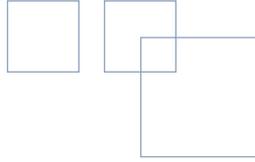
3

Provide the warfighter an assured information environment, protected and defended throughout the battlespace and across the entire network.

The essential elements of IA include protecting information, defending the network and keeping network services available. This is done by acquiring trusted software, providing integrated situational awareness, transitioning and enabling IA capabilities and creating an IA-empowered workforce. Assured information is required in all mission areas (e.g., warfighter, intelligence and business).

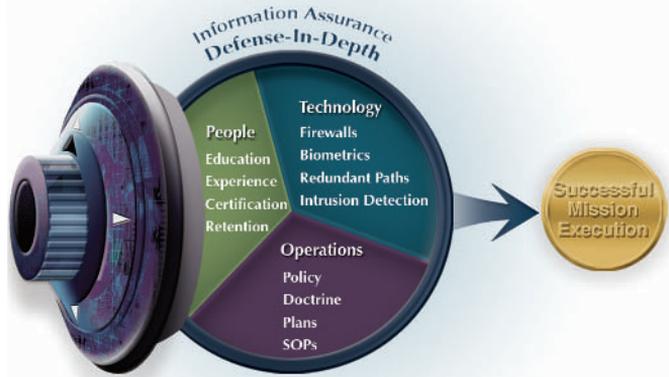
Goal 3 Intent:

To meet the challenges of ensuring appropriate protection of information during transmission, processing and storage, the development and publication of DOD-level strategies and guidance are necessary to strengthen and synchronize DOD efforts to secure the network. Key to this effort is the development of a National Military Strategy for Cyberspace Operations (NMS-CO). The NMS-CO provides a comprehensive plan for DOD orchestration of national military strategic actions needed to operate in cyberspace and increase trust and confidence in its ability to dominate in cyberspace. Additionally, DOD-level guidance is required to address IA certification and accreditation; GIG policy, responsibilities and processes; IA controls; and critical infrastructure protection (CIP) measures.



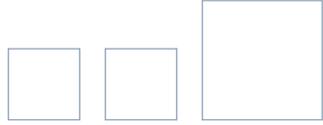
Establishing GIG computer network defense (CND) capabilities that support protecting, monitoring, detecting, analyzing and responding to unauthorized activity and unintentional user errors will provide the Department of Defense with the capability to resist and, if necessary, respond to attack. The required capability will enable rapid recognition, recovery and response to attacks or events affecting the network and/or information resources, with the ultimate goal of ensuring the continuity of access and use by authorized personnel. To achieve this capability, the Department must develop a CND CONOPS and acquire, field and establish tools that bridge the current CND capability gaps. Additionally, it is necessary to field upgraded IA software and hardware.

Beyond technical solutions, the development of a professional CND workforce through improved training, doctrine, TTPs and exercises is vital. It is necessary to train personnel in all aspects of IA across the combatant commands, Services and agencies. Incorporation of IA and CND in exercise planning and execution improves effective evaluation of DOD capabilities and promotes realistic training for IA professionals, commanders and senior leaders and will lead to the development of necessary TTPs. This training needs to include the ability to facilitate IA workforce



proficiency between exercise opportunities. The joint community must also place a greater emphasis on ensuring IA positions are filled with joint certified personnel.

Defining new encryption and data technologies and procedures to maintain the confidentiality and integrity and/or non-repudiation of information and provide highly available ES is paramount in today's environment. Consolidation of communications security (COMSEC) management, distribution and training into a joint standard is necessary to alleviate disparate COMSEC management procedures across the Services. Integrating CIP measures into programming and operational processes will ensure ES are available for warfighter operations. Modernized encryption and data technologies must be addressed to enhance confidentiality and integrity and/or non-repudiation.



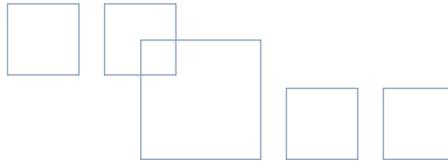
The joint community must establish methods and measures of effectiveness (MOE) to identify and periodically assess our ability to secure the network. Building a comprehensive set of IA/CND metrics that measures the strategic health of the network is necessary to provide a DOD-wide operational picture of our IA/CND posture and react to shortfalls. The joint community must institutionalize the collation and analysis of DOD IA/CND assessment activities.

Acquisition strategies must be modified to improve network security through system assurance measures. Most DOD capabilities depend on systems developed in the commercial sector. These systems have high operational impact on the defense of our Nation and protecting critical infrastructure at home and abroad. Guidance and processes must be developed that actively ensure DOD systems are delivered with the highest level of inherent security.

The Department of Defense must improve processes that provide shared situational awareness and monitor the performance, operational status and security of the GIG. Measures to protect critical infrastructure must include standard reporting procedures so that those who manage and defend portions of the network contribute to a common understanding of the status of the entire GIG. The establishment of processes, procedures and corrective actions through the use of a DOD-wide operational picture will help ensure GIG integrity, which will positively impact warfighter operations.

Goal 3 Objectives:

- 3.1 Develop strategies and guidance to strengthen and synchronize DOD efforts to secure the network.
- 3.2 Establish GIG CND capabilities that support protecting, monitoring, detecting, analyzing and responding to unauthorized activity and unintentional user errors.
- 3.3 Develop a professional CND workforce through improved training, doctrine, TTPs and exercises.
- 3.4 Define new encryption and data technologies and procedures to maintain the confidentiality and integrity and/or non-repudiation of information and provide highly available ES.
- 3.5 Establish methods and MOE to identify and periodically assess DOD ability to secure the network.
- 3.6 Develop acquisition strategies that improve network security through system assurance measures.
- 3.7 Assess and improve procedures and processes required to maintain shared situational awareness and monitor the performance, operational status and security of the GIG.



Goal 4 – Accelerate Information Sharing

4

Develop a strategy that supports cross-mission area and cross-domain information sharing throughout the battlespace.

The combatant commanders' requirement to securely share information with mission partners has been highlighted in lessons learned, in actions ranging from MCO in Iraq to humanitarian assistance for relief in the wake of international and domestic disasters such as the Indian Ocean tsunami and Hurricanes Katrina and Rita. Information sharing requires a strong foundation provided by clear policy, comprehensive data strategy, common ES, robust infrastructure and institutionalized IA capabilities.

In January 2006, the DOD CIO was appointed the single focal point within the Department for information sharing policy and implementation guidance. The Joint Staff is partnering with the Office of the ASD(NII) to develop an information sharing strategy that addresses sharing with US government departments and agencies, the IC, state and local governments and other mission partners. Development of this strategy was also directed by the *2006 QDR Report*.

Goal 4 Intent:

The Department of Defense must establish an information sharing environment. A key component of this is the development

of a DOD information sharing strategy to address policy, processes, procedures, standards and CONOPS for the sharing of critical information with joint, multinational, interagency and inter-governmental mission partners. Relevant common operational pictures and improved DOD or interagency standards for the classification and transfer of information will advance our ability to share information.

A KM capability is necessary to further advance information sharing. Many organizations inside and outside of the Department of Defense are working on facets of KM, but no central effort is currently underway within the Department to refine and standardize the military application of this function.

The Department must accelerate the development of CDS capabilities. Establishment of a cross-domain management office (CDMO) will help unify efforts and accelerate and streamline the development, certification, evaluation and testing of potential CDS.

In order to improve multinational information sharing (MNIS) the joint community must sustain current operational systems, transition to an enterprise architecture and support the development of an objective information sharing capability.

Goal 4 Objectives:

- 4.1 Establish a DOD and interagency information sharing environment that includes common standards, architecture and culture.



- 4.2 Refine KM capabilities required across the DOTMLPF spectrum and publish results in appropriate doctrine, policy, or concept document.
- 4.3 Accelerate the development of CDS to move information across security classification and national boundaries by consolidating program efforts and refining certification and accreditation processes.
- 4.4 Improve MNIS capability by sustaining current operational systems, transitioning to an enterprise architecture and supporting the development of objective information sharing capability.

Goal 5 Intent:

The *2006 QDR Report* provides direction to accelerate the transformation of the Department of Defense, to focus more on combatant commanders' required capabilities and to develop portfolios of joint solutions rather than individual Service-centric programs. JNO is specifically identified as one of three "first-step" capability-managed portfolios. Current JNO efforts are being executed as independent acquisition programs under separate acquisition processes and milestone decision authorities (MDAs). A governance and management structure must be established to facilitate the development and integration of these core programs so that they provide a common, core infrastructure to support future joint operations. The materiel and non-materiel elements of JNO capabilities must be developed in a synchronized and integrated way. The delivery of JNO capabilities requires new approaches as the joint community leverages the three major DOD processes: requirements (capabilities), resourcing and acquisition. To optimize capability delivery, a "centralized" management process is needed that allows for trades and balancing not only within each process, but also among them.

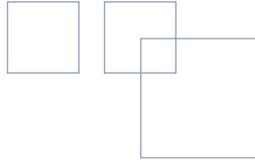
To advance communication system engineering and integration, the GIG architectures and standards must be synchronized with the Joint Capabilities Integration and Development System (JCIDS) and Information Support Plan (ISP) assessment processes and the modeling, simulation and testing environments. To accomplish this, the DOD CIO will continue

Goal 5 – Synchronize Delivery of Network Capabilities

5

Strengthen joint warfighting by synchronizing delivery of capabilities and ensuring integration of capabilities across the entire DOTMLPF.

To exploit the full power of information, the joint community needs a synchronized approach to developing, procuring, engineering and fielding joint capabilities. Ongoing efforts in system engineering, interoperability and supportability, certification, portfolio management, operational testing, capability-based assessment (CBA), common lexicon development and training are contributing to achieving this synchronized approach.



to provide policy and oversight while the entire joint community assists DISA in executing its role as the GIG end-to-end (E2E) systems engineering (SE) implementer.

A JNO test environment is needed to provide realistic testing and evaluation and to institutionalize common tools, interfaces and network capabilities. The many disparate test networks (e.g., Defense Research and Engineering Network (DREN), DISN-Leading Edge Services (LES) should be merged into DOD-wide standard test facilities and capabilities.

Joint programs for modeling and simulation (M&S) are needed to provide communications planners and system analysts with the capability to validate support plans, analyze existing and proposed network architectures and predicatively evaluate the performance of new devices and applications. Common communications system M&S tools are needed to improve joint communications planning and execution.

Information technology (IT) portfolio management is the emerging process that assesses groups of systems to improve IT and National Security Systems (NSS) investment decisions. The warfighting mission area (WMA) IT portfolio investment analysis should provide prioritization and integration recommendations to the capabilities, acquisition and budget process decision makers. The IT portfolio management process must be synchronized and integrated with JCIDS, Defense Acquisition System (DAS) and the planning, programming,

budgeting and execution (PPBE) process to improve decisions on individual IT and NSS investments.

To professionalize JNO, the joint community must develop a comprehensive joint training program. The community must institutionalize its body of knowledge and facilitate and/or advocate training for the joint personnel who plan, install, manage, operate and protect joint networks. A central location for information on detailed mission, content and oversight of joint and Service curriculum is also needed. Training opportunities summarized and published in a joint directive would also benefit warfighting operations.

The joint community must employ a rigorous and repeatable analytical process to improve capability assessments and gap analysis. Additionally, the joint community must also be educated in the use of JCIDS and establish guidelines for the application of emerging analysis information and tools.

Multinational interoperability is a critical enabler to seamless, reliable JNO. An improved process is needed to collaborate with multinational mission partners to





develop and implement IT standards that promote interoperability.

Goal 5 Objectives:

- 5.1 Advance system engineering and integration to improve interoperability and supportability of IT and NSS.
- 5.2 Complete initial NCOE efforts to define capabilities for first tactical mile users and leverage this work to create a portfolio management concept for integrated capability delivery based on an enterprise-wide JNO taxonomy.
- 5.3 Create a JNO test environment for joint, multinational, interagency and inter-governmental testing.
- 5.4 Define common M&S tools that support and enable JNO.
- 5.5 Manage the WMA IT portfolio investment analysis to provide prioritization and integration recommendations to the capabilities, acquisition and budget process decision makers.
- 5.6 Advocate training for joint personnel to enhance JNO.
- 5.7 Employ a rigorous and repeatable analytical process to improve capability assessments and gap analysis.
- 5.8 Collaborate with allied and coalition partners to develop and implement policies, procedures and IT standards that promote combined interoperability.

Goal 6 – Transform GIG Enterprise Management and Enhance Electromagnetic Spectrum Access

6

Support JNO through improved GIG enterprise management, including electromagnetic spectrum management at all echelons.

The NetOps operational construct consists of situational awareness (SA), C2 and the essential tasks. NetOps is the organizations and procedures required to operate and defend the GIG. NetOps is an integrated approach to accomplishing the three interdependent essential tasks—GEM, GND and IDM/CS. NetOps is orchestrated by USSTRATCOM through JTF-Global Network Operations (GNO) and provides a NM system that delivers E2E services, GIG SA, protection and control. NM focuses on the people, technology, processes, policy and capabilities necessary to effectively operate systems and networks, including their configuration, availability, performance, manageability and enterprise connectivity. Configuration management (CM) must be integrated throughout the entire network lifecycle, ranging from the research and development effort to the retirement of JNO capabilities.

Transformation of GIG management to support JNO is important to meet the transformational warfighting concepts in support of our armed forces. The electromagnetic spectrum is a finite natural resource controlled by sovereign entities.



Challenges such as host nation spectrum coordination and approval, worldwide electromagnetic spectrum reallocation, increased commercial competition and the international frequency assignment process make access to sufficient electromagnetic spectrum to support military operations problematic. Spectrum management, a subset of GEM, is of growing concern. There has been an explosive increase in worldwide demand for electromagnetic spectrum access for both civil and military use. Careful management of electromagnetic spectrum access is vital to support current and future military operations.

Goal 6 Intent:

The NetOps capability requires continued emphasis. The joint community must develop a policy and governance structure that facilitates E2E enterprise management. We must continue to refine the NetOps CONOPS and improve GIG SA and defense capabilities. We must encourage the use of common and compatible tools sets for GEM and GND and develop a common data strategy to enable GIG IDM/CS. Additionally, we need to explore ways to provide a better combatant command and JTF-centered view of the network.

It is essential that the Department of Defense move toward solutions for GEM that are compatible with other GIG systems and DOD policy. The joint community should support the NCOE (now called JNO) tasks that attempt to bring together, under one program office, several of the major GIG programs of record. Additionally, we must support ongoing GIG SE efforts that will put into place the tool sets required to accomplish GEM.

The joint community must continue to: advocate the development of electromagnetic spectrum-dependent equipment that is usable in required operational environments; support enforcement of national and international guidelines; protect current DOD electromagnetic spectrum allocations against encroachment; and refine electromagnetic spectrum management policy. There is a need to improve education and awareness throughout the operational and acquisition communities on the criticality of electromagnetic spectrum resources.

Further joint policy and standards are needed for management and use of the electromagnetic spectrum, including CM. Electromagnetic spectrum management is currently the responsibility of the individual Military Departments (MILDEPs) within the United States and its possessions and by the geographic combatant commands outside of the United States and its possessions. To accommodate future responsibilities of US Northern Command (USNORTHCOM) within the United States, as well as multinational mission partners, the electromagnetic spectrum management process needs to be re-evaluated. Currently, there are only Service single-focus tools to meet joint requirements. A comprehensive net-centric electromagnetic spectrum tool suite is required to support the objectives of transformation and future joint operations.

The joint community must also establish a standardized electromagnetic spectrum management capability to support the Department of Defense, multinational, interagency and inter-governmental



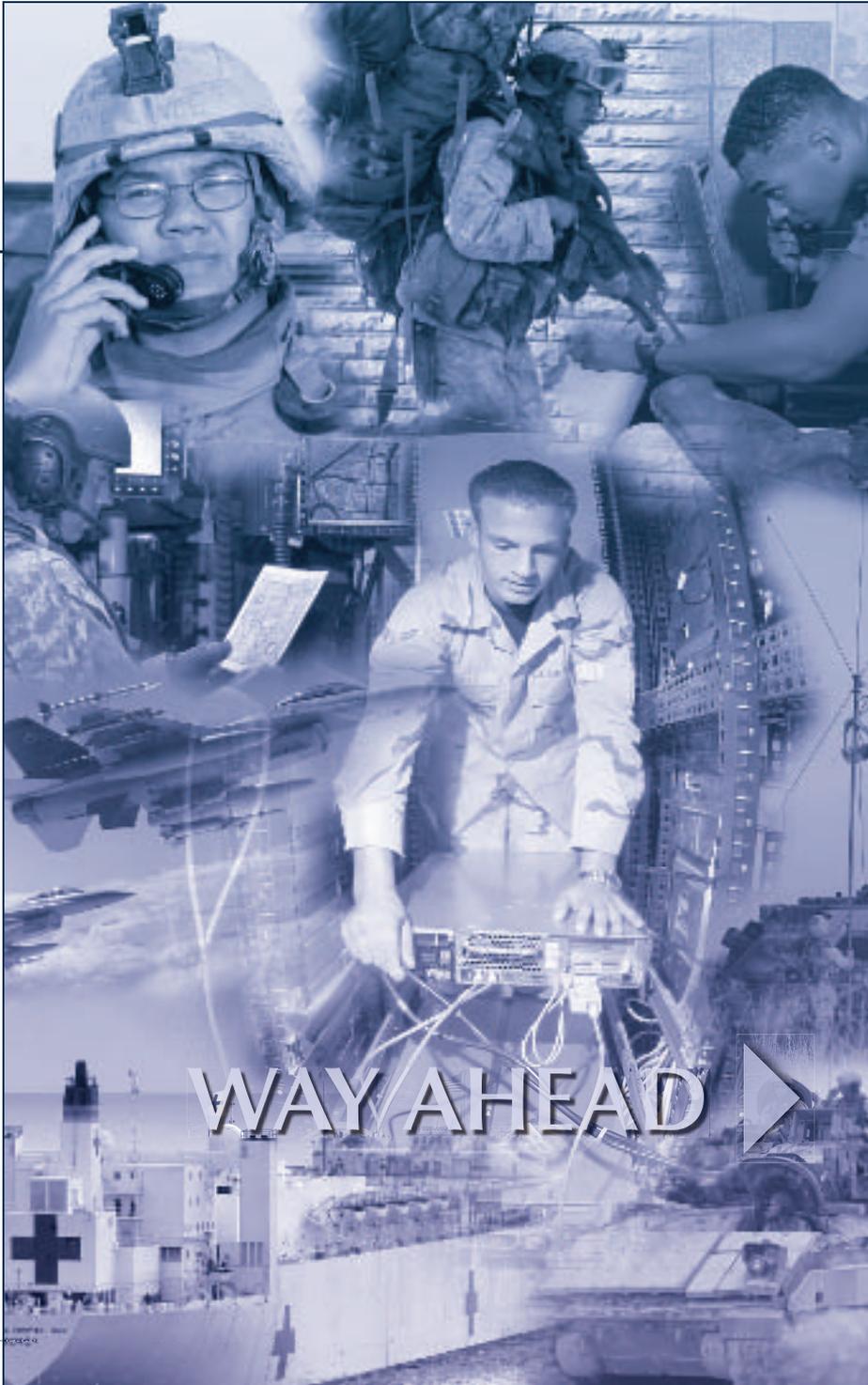
DOD Electromagnetic Spectrum Use

operations. Additionally, a cadre of professional electromagnetic spectrum management personnel (military and civilian) must be developed who are capable of meeting the electromagnetic spectrum demands across the entire continuum of operations.

Goal 6 Objectives:

- 6.1 Develop policy and governance structure to facilitate E2E enterprise management.
- 6.2 Advocate enterprise management capabilities and solutions congruent with direction of emerging DOD policy and guidance.

- 6.3 Promote electromagnetic spectrum access and awareness for DOD forces operating in joint, multinational, interagency and inter-governmental environments.
- 6.4 Establish a standardized electromagnetic spectrum management capability to support DOD, multinational, interagency and inter-governmental operations.
- 6.5 Develop a cadre of professional electromagnetic spectrum management personnel (military and civilian) capable of meeting the electromagnetic spectrum demands across the continuum of operations.



WAY AHEAD ▶

The joint community has made significant progress since the publication of the Joint C4 Campaign Plan in September 2004. We have re-emphasized joint communications “basics” and actively framed issues around operational support to the warfighter; we have also improved understanding of JNO capabilities within the operational community.

This JNO Campaign Plan is a living document that provides a strategy for the next 2 to 5 year period to move toward achieving the full potential of JNO capabilities outlined in transformational concept and capabilities documents. Goals and objectives cover actions that must be taken across the DOTMLPF. The effort to create an NCE continues to prove a difficult and far-reaching challenge in its sheer scope, complexity and number of interdependencies.

The true impact of this campaign plan and way ahead will be the joint community collective efforts in implementing the actions identified in Annex A.

As stated in the *DOD National Defense Strategy*, “Transforming to a net-centric force requires fundamental changes in processes, policy and culture. Changes in these areas will provide the necessary speed, accuracy and quality of decision-making critical to future success.” Cultural challenges to transforming the force continue to be the hardest ones we face. The joint communications community must work together to ensure the Department of Defense gets it right. The warfighting community is counting on the full combat power across the full continuum of operations that networked joint capabilities bring to the fight.





ANNEX A



In order to facilitate keeping the plan as a living document, the JNO Campaign Plan is published in hardcopy without the action item lists. This section contains an abbreviated version of Annex A providing an overview of the goals, objectives and objective details. The complete version of Annex A to include the action item list is located on the Joint Staff website at <http://www.jcs.mil/j6/jointcampaign.html>.

Goal 1: Connect the Warfighter

- **Objective 1.1:** Develop Strategies for Warfighters Beyond Line-of-Sight Needs to Include a Balance Between Military and Commercial SATCOM and Alternatives to Space-Based Capabilities

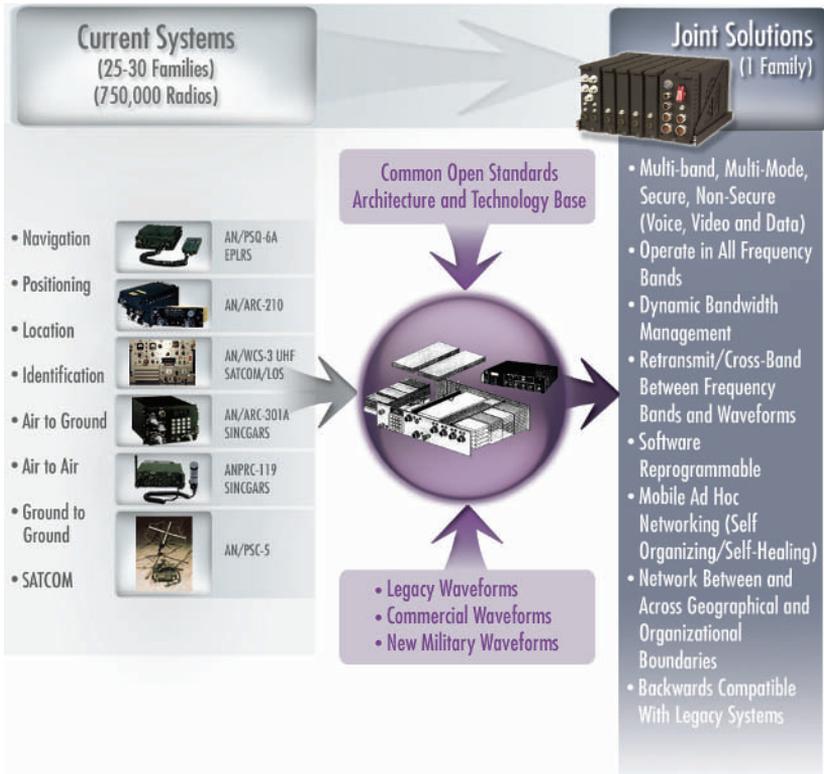
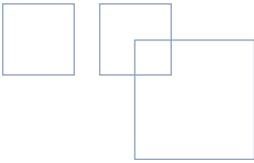
Joint Staff Division Lead: J-6C

The community needs to partner with all relevant organizations to ensure programs meet joint capability requirements, remain on-schedule and control costs. In addition, the community must continue to research and advocate for technologies that possess military application. Identification and evaluation of new technologies must include technology readiness level, cost-benefit and risk assessments. The community must also analyze commercial and military SATCOM needs as well as conduct a review of all satellite requirements to ensure the accuracy of the SATCOM database (SDB).

- **Objective 1.2:** Orchestrate Collection, Validation and Implementation of Joint Warfighting Capabilities Into Existing Information Infrastructure and the DISN

Joint Staff Division Lead: J-6C

Transition to the new DISN infrastructure requires the formal documentation of various processes. Additionally, the community must support secure and seamless communication with non-DOD agencies, especially in times of crises and comply with Presidential directives regarding information sharing.



Joint Tactical Radio System (JTRS)

- **Objective 1.3:** Develop Joint Wireless Capabilities to Support JNO

Joint Staff Division Lead: J-6C

Joint wireless capabilities will connect tactical units to the GIG, enabling mission partners to share near-real-time voice, data and video communications. To facilitate the development and deployment of wireless capabilities, CONOPS and interoperability standards need to be created and new technologies (such as the Joint Tactical Radio System

(JTRS), an IP-based, software definable radio set) need to be fielded.

- **Objective 1.4:** Resolve Interoperability and Integration Issues Occurring Within the Operational Environment

Joint Staff Division Lead: J-6I

Lessons learned from recent operations and DOD exercises provide critical feedback on system interoperability. OSD Operational Test and Evaluation Directorate (DOT&E) and Joint Staff/J-6



will team to provide interoperability assessments during annual C/S/A-sponsored exercises and identify shortfalls.

- **Objective 1.5:** Develop and Enforce Compliance of GIG Implementation Guidance to Enable JNO, Integration and Data Sharing in Connecting to the GIG Enterprise

Joint Staff Division Lead: J-6I

GIG key interfaces are critical to the enterprise. Two important initiatives are KIP development and NCIDs. The KIP Transport Family Version 1.0 is complete and ASD(NII) is developing NCIDs as systems engineering guidance. Data sharing is equally important to connecting the warfighter. DOD implementation of the Net-Centric Data Strategy (NCDS) will enable information sharing capabilities and ensure operationally effective information exchanges.

- **Objective 1.6:** Maximize Support to Combatant Commanders Through Joint Programs, Processes and Venues to Meet Rapidly Evolving JNO Operational Requirements

Joint Staff Division Lead: J-6A/Z

According to the 2006 QDR Report, the Department of Defense's current structure and processes are handicaps in the protracted fight against agile and networked foes. In order to maximize support to combatant commanders, the joint community must make better use of available tools and technology to respond to emerging warfighter needs.

- **Objective 1.7:** Develop a Strategy and Validate Performance Testing With Delivery of Essential Network Services During DOD Migration to IPv6

Joint Staff Division Lead: J-6C

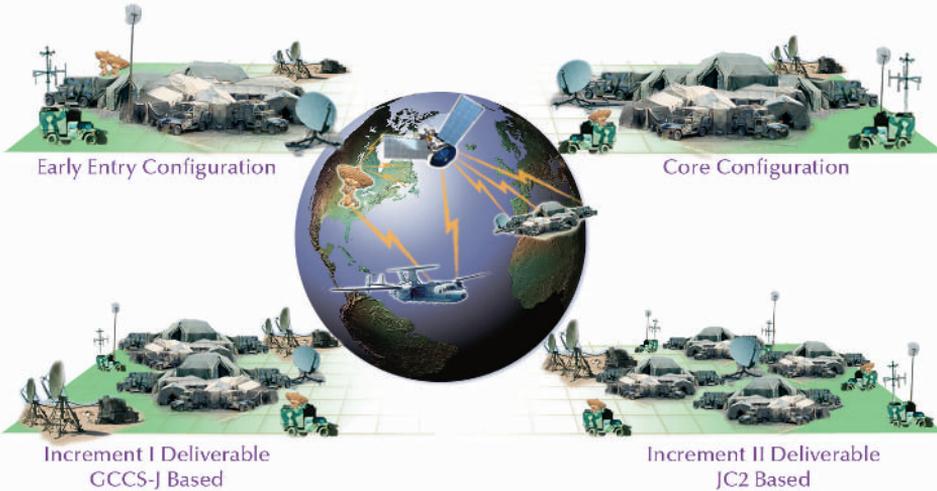
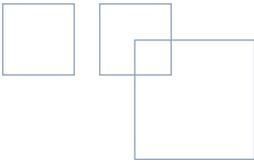
The transition to IPv6 will be a gradual, market-based process. Industry's development, testing and distribution of IPv6 standards, equipment and services will dictate the pace of transition. The joint community must continue to support development of DISA's Master Test Plan, DISA and Service IPv6 implementation plans and capabilities to better understand the technical aspects of "IPv6 capable." As IPv6 continues to mature, the joint community must identify potential technical implementation issues, policy and doctrine implications and network management considerations.

Goal 2: Leverage the Power of Enterprise Services

- **Objective 2.1:** Develop Strategies, Facilitate Enabling Policy and Provide Joint Guidance in Support of DOD Efforts to Transition to ES

Joint Staff Division Lead: J-6C

To realize net-centricity, the Joint Staff, C/S/As and the IC must work together to define, establish and synchronize requirements, policy and strategies to ensure that the future JNO supports evolving operational requirements. Key efforts include the Department of Defense working to: strengthen data strategies; develop an information sharing strategy with federal, state, local and coalition



Deployable Joint Command and Control (DJC2) Deployment Phases

partners; and synchronizing net-centric investment portfolios.

- **Objective 2.2:** Establish and Advocate Net-Centric Enterprise Service Capabilities Required to Support JNO

Joint Staff Division Lead: J-6C

To realize net-centricity, the Joint Staff, C/S/As and the IC must work together to define, establish and synchronize operational requirements in the NCE.

- **Objective 2.3:** Facilitate the Transition and Integration of DOD C2 and/or Shared Situational Awareness Efforts Into a Net-Centric Enabled Environment

Joint Staff Division Lead: J-6C

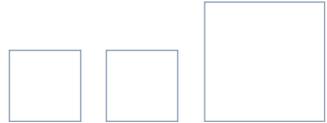
The Joint Staff/J-6 will monitor the NECC TD phase to ensure that the migration of Global Command and Control System-Joint (GCCS-J) capability continues to

provide appropriate IA, in accordance with the designated approval authority role of Joint Staff/J-6. Careful monitoring of NECC development during the TD phase is also necessary to assess the synchronization of the NECC enterprise service requirements with the NCES CES capability.

- **Objective 2.4:** Develop Policy, Procedures and Solutions to Ensure ES Capabilities are Sufficient and Available to Meet the Rapid Deployment and Employment of a JTF

Joint Staff Division Lead: J-6C

The community must continue to define functional, organizational and operational requirements for deployed joint C2 initiatives and programs of record. The 2006 QDR Report called for the transformation of designated Service operational headquarters to fully



functional and scalable joint C2 JTF-capable headquarters beginning in FY 2007. This new guidance may influence current joint programs of record, such as the DJC2 System and incorporate new initiatives such as USJFCOM's "Turnkey Solution for Joint Headquarters." The Joint Staff/J-6 must stay engaged in the ongoing process to determine future deployed C2 solutions for the joint warfighter.

Goal 3: Secure the Network

- **Objective 3.1:** Develop Strategies and Standardize Guidance to Strengthen and Synchronize DOD Efforts to Secure the Network

Joint Staff Division Lead: J-6X

Establishes DOD-level strategy and guidance to ensure appropriate protection of information during transmission, processing and storage. Protection is required for the level of risk, loss, or harm that could result from disclosure, loss, misuse, intentional or inadvertent destruction, or non-availability of DOD information. One key to this objective is the development of an NMS-CO. The NMS-CO provides a comprehensive plan for the Department of Defense to orchestrate national military strategic actions needed to operate in cyberspace and ensure trust and confidence in cyberspace.

- **Objective 3.2:** Establish GIG CND Capabilities That Support Protecting, Monitoring, Detecting, Analyzing and Responding to Unauthorized Activity and Unintentional User Errors

Joint Staff Division Lead: J-6X

Develop the capability to resist attack and to rapidly recognize, recover and respond to attacks on the network and to information resources, ensuring the continuity of access and use by legitimate users. Establish common DOD-wide IA tool suites and capabilities to support C/S/A efforts. Work with the Enterprise Solution Steering Group (ESSG) to allocate fenced IA funds to meet critical DOD shortfalls.

- **Objective 3.3:** Develop a Professional CND Workforce Through Improved Training, Doctrine, TTPs and Exercises

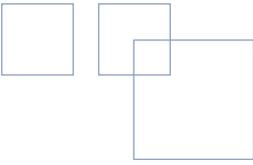
Joint Staff Division Lead: J-6X

Beyond technical solutions, it is vital to train personnel in all aspects of IA across the C/S/As. Incorporation of IA and CND in exercise planning and execution ensures effective evaluation of DOD capabilities and promotes realistic training for IA professionals.

- **Objective 3.4:** Define New Encryption and Data Technologies and Procedures to Maintain the Confidentiality and Integrity and/or Non-Repudiation of Information and Provide Highly Available ES

Joint Staff Division Lead: J-6X

The consolidation of COMSEC management, distribution and training into a joint standard will alleviate disparate COMSEC management procedures across the Services. Integrating CIP into operational processes will ensure highly available enterprise services are on hand for key



warfighter operations. Modernized encryption and data technologies are required to enhance confidentiality and integrity and/or non-repudiation. Operational necessities, current and projected, demand IA solutions and their infrastructures achieve this transformation, while simultaneously overcoming algorithm aging and logistics sustainability issues.

- **Objective 3.5:** Establish Methods and Measures of Effectiveness to Identify and Periodically Assess DOD Ability to Secure the Network

Joint Staff Division Lead: J-6X

Build a comprehensive set of IA and CND metrics that measure the strategic health of the network. These activities will result in the ability to provide a DOD-wide picture of our IA and CND posture and react to shortfalls. To best assess IA, the community must institutionalize the collation and analysis of DOD IA and CND assessment activities. The results of the assessments must be considered and folded into DOD decision-making processes.

- **Objective 3.6:** Develop Acquisition Strategies That Improve Network Security Through System Assurance Measures

Joint Staff Division Lead: J-6X

Software and hardware assurance relates to the level of confidence felt in software applications and the hardware platforms that run them; that they function as intended and are free of vulnerabilities, either intentionally

or unintentionally designed or inserted during the lifecycle. System assurance describes the combination of both software and hardware assurance. Most US DOD capabilities depend on systems developed in the commercial sector. These systems are mission critical not only for the DOD prime mission of securing our Nation, but also for protecting critical infrastructure at home and abroad. US enemies (including nation states, terrorists, criminals and rogue software and hardware developers) may gain control of DOD systems through supply-chain opportunities (intentionally embedding malicious code) or by remotely exploiting software that is vulnerable through quality defects. As the Department acquires, manages and employs complex, software-intensive systems, it must manage the risks associated with these vulnerabilities. Ultimately, the Department needs an acquisition process that allows decision makers to balance system risk (threat) with affordability, technical feasibility and operational capability.

- **Objective 3.7:** Assess and Improve Procedures and Processes Required to Maintain Shared Situational Awareness and Monitor the Performance, Operational Status and Security of the GIG

Joint Staff Division Lead: J-6Z

Standardized reporting procedures and processes are necessary so that everyone who manages and defends the network can achieve a common understanding of the status of the GIG.



Goal 4: Accelerate Information Sharing

- **Objective 4.1:** Establish a DOD/ Interagency Information Sharing Environment That Includes Common Standards, Architecture and Culture

Joint Staff Division Lead: J-6X

It is necessary to codify the specific warfighting information sharing requirements, policies, culture and material solutions as prerequisites to the effective implementation of the National Security Strategy and National Response Plan. A key component of this is the development of a DOD/interagency information sharing environment to address policy, processes and procedures for the sharing of critical information with joint and interagency partners. Without an articulate, robust strategy, interoperable and interdependent capabilities will not be realized.

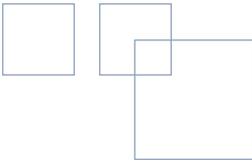
- **Objective 4.2:** Refine KM Capabilities Required Across the DOTMLPF Resource Spectrum and Publish Results in Appropriate Doctrine, Policy, or Concept Document

Joint Staff Division Lead: J-6A

In order for JNO to create warfighting effects, the NCOE JIC and current JCA effort define a new Tier 2 capability set for KM. KM is defined as “the systematic process of discovering, selecting, organizing, distilling, sharing, developing and using information in a social domain context to improve warfighter effectiveness.” KM stems from the premise that an organization’s

competitive advantage exists in how well and how widely that organization uses and enhances its own collective knowledge. Improvement to technical networking capabilities alone, while desirable, amount to little more than “better comms.” In order for the network to create new effects and thereby achieve the truly transformational capabilities envisioned by the “GIG” construct, the network must rapidly respond to ever changing operational priorities and needs. While future network managers will have tools to dynamically allocate network resources such as bandwidth, a mechanism is needed to bridge the current gap between rapidly changing mission needs and the priorities network managers follow to meet these needs. This mechanism is a set of tools and techniques collectively referred to as KM. Many organizations inside and outside of the military are working on various facets of KM, but no central effort is currently underway within the Department of Defense to discover, refine and standardize the military application of this new function. Over the next 2 to 5 years, it is critical that the Department establish a process to rapidly apply emerging commercial tools and techniques through experiments and other pathfinder efforts and then determine a means to standardize these and conduct the necessary joint force-wide training to make effective use of this new capability area.

- **Objective 4.3:** Accelerate the Development of CDS to Move Information Across Security Classification and



Long-Term Objectives

- Exportable and Affordable Technologies
- Platform and Transport Agnostic Information Exchange
- Consumable Service Between Mission Partners
- Adaptive Distributed Global Network
- Dynamic Releasable Information
- Collaborative Work Environment

Future Information Sharing Concept

National Boundaries by Consolidating Program Efforts and Refining Certification and Accreditation Processes

Joint Staff Division Lead: J-6X

The Department of Defense and IC require the CDMO to accelerate the development, certification, evaluation and testing of potential cross-domain solutions. The CDMO will leverage like requirements, technology and funds for a more efficient process of CDS development between the Department and the IC.

■ **Objective 4.4:** Improve MNIS Capability by Sustaining Current Operational Systems, Transitioning to an Enterprise Architecture and Supporting the Development of Objective Information Sharing Capability

Joint Staff Division Lead: J-6X

It is necessary to codify the specific warfighting information sharing requirements, policy, culture and material solutions as a precursor to the implementation of the National Security Strategy and National Response Plan.



Goal 5: Synchronize Delivery of Network Capabilities

- **Objective 5.1:** Advance Communication System Engineering and Integration to Improve Interoperability and Supportability of IT and NSS

Joint Staff Division Lead: J-6I

The ASD(NII)/DOD CIO E2E SE Advisory Activity is realigning its responsibilities with the newly stood-up DISA E2E SE office. The DOD CIO provides policy and oversight, while the joint community assists DISA with the GIG E2E SE implementation and technical standards documentation. GIG architectures and standards must be synchronized with the JCIDS and ISP assessment processes and the modeling, simulation and testing environments.

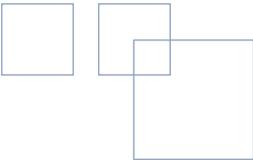
- **Objective 5.2:** Complete Initial NCOE Efforts to Define Capabilities for First Tactical Mile Users and Leverage This Work to Create a Portfolio Management Concept for Integrated Capability Delivery Based on an Enterprise-Wide JNO Taxonomy

Joint Staff Division Lead: J-6A

A tiger team was formed in 2004 to identify the challenges in fielding critical enabling network (e.g. NCOE) capabilities and to develop potential options to deliver synchronized capabilities. In February 2005 the Joint Chiefs of Staff endorsed the NCOE Project way-ahead, directing the development of an NCOE JIC with illustrative CONOPS; development of

a strategy, terms of reference (TOR) and implementation roadmap; and review and assessment of management and governance options for achieving the NCOE. The NCOE JIC received JROC approval in October 2005 and a subsequent Net-Centric Functional Capabilities Board (NCFCB) led CBA is scheduled for completion in 2006 with approval of a Joint Capabilities Document (JCD). ASD (NII) has completed the implementation roadmap and TOR. When combined with the NCOE JCD, these efforts will provide an initial analytical foundation for net-centric capabilities.

As a result of the 2006 QDR Report guidance to develop joint capability portfolios, the Deputy's Advisory Working Group (DAWG) directed a JNO portfolio management experiment with ASD(NII) and Commander, USSTRATCOM, assigned as co-leads. This effort is anticipated to complete the work initiated under the NCOE project to develop management and governance options for synchronized capabilities delivery. This broad initiative will expand the warfighter-focused NCOE work into enterprise-wide capabilities-based planning recommendations using the JNO lexicon and taxonomy developed under the JCA initiative. Version 2 of the JNO Joint Functional Concept will further mature and expand the JNO lexicon and taxonomy to provide a common, community-wide vocabulary and further define joint net-centric operations environment capabilities and lessons learned from the CBA.



- **Objective 5.3:** Create a Net-Centric Operations Test Environment for Joint, Multinational, Interagency and Inter-Governmental Testing

Joint Staff Division Lead: J-6I

The net-centric test environment will institutionalize common tools, interfaces and network capabilities to provide realistic testing and evaluation in a joint operational context. The Department of Defense requires a persistent testing, modeling and simulation capability to facilitate evaluation of net-centricity early and throughout a program's development cycle. The Joint Staff/J-6 supports OSD efforts to build standard test facilities and capabilities as it leads DOD efforts to merge the many disparate test networks (e.g., DREN, DISN-LES) into a seamless DOD-wide enterprise.

- **Objective 5.4:** Define Common M&S Tools That Support and Enable JNO

Joint Staff Division Lead: J-6C

Network Warfare Simulation (NETWARS) is the joint communications M&S program. It is being developed by DISA, in conjunction with Joint Staff/J-6, to provide communications planners and analysts with the capability to validate communications support plans, analyze existing and proposed network architectures and predicatively evaluate the performance of new communications devices and applications. NETWARS is being socialized with the Services and combatant commands as the common M&S tool.

- **Objective 5.5:** Manage the WMA IT Portfolio Investment Analysis to Provide Prioritization and Integration Recommendations to the Capabilities, Acquisition and Budget Process Decision Makers

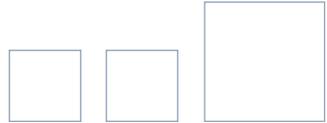
Joint Staff Division Lead: J-6I

Joint Staff/J-6 will use IT portfolio management (PFM) to improve IT and NSS investment decisions by objectively assessing individual systems as groups of investments. In completing this work, J-6 will improve synchronization of JCIDS, DAS and PPBE decisions concerning individual IT and NSS investments. There will be opportunities to reduce duplicative IT and NSS efforts and re-invest resources for other capabilities. IT PFM will allow objective assessments and prioritization of IT and NSS systems within the IT domain portfolios. Finally, J-6 will facilitate better IT and NSS management of data collection, distribution and use across the Joint Staff.

- **Objective 5.6:** Advocate Communication Systems Training for Joint Personnel to Enhance JNO

Joint Staff Division Lead: J-6 DAG

The impact of JNO continues to exceed the training requirements of combatant and JTF commanders. Current efforts, ranging from enhancing spectrum management to developing the Joint C4 Planners Course, address existing voids. Ensure existing training presents the appropriate content and possesses the correct oversight to best serve the joint force. Look to present actions and



potential engagements to both update today's training and develop new opportunities.

- **Objective 5.7:** Employ a Rigorous and Repeatable Analytical Process to Improve Capability Assessments and Gap Analysis

Joint Staff Division Lead: J-6A

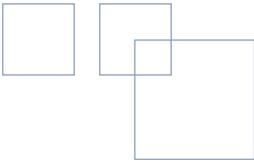
Both JCIDS and the application of JCIDS analysis tools within the NC FCB continue to evolve. Even as awareness, acceptance and use of JCIDS spreads, the shortfalls in application of the processes, particularly with respect to the ability to make rigorous capability-trade recommendations, are increasingly problematic. To address these shortfalls, Joint Staff/J-6A will initiate two new efforts: 1) educate the NC FCB stakeholders on the use of JCIDS; and

2) establish guidelines for capability portfolio assessments using emerging analysis information and tools.

- **Objective 5.8:** Collaborate With Allied and Coalition Partners to Develop and Implement Policies, Procedures and IT Standards That Promote Combined Interoperability

Joint Staff Division Lead: J-6B

Combined interoperability is a critical enabler to seamless, reliable, net-centric operations. Improving combined interoperability of data, applications and systems is paramount. Combined interoperability does not happen by chance; it has to be planned and paid for, up-front. Steps taken in recent years are improving combined interoperability, but much work remains.



Goal 6: Transform GIG Enterprise Management and Enhance Electromagnetic Spectrum Access

- **Objective 6.1:** Develop Policy and Governance Structure to Facilitate E2E Enterprise Management

Joint Staff Division Lead: J-6C

ASD (NII), Joint Staff/J-6, USSTRATCOM and JTF-GNO will continue to refine and develop NetOps policy, guidance and TTPs along with GIG C2, SA and defense capabilities. Control and visibility of the GIG is currently Service-centric; move toward a regional combatant command-centric view. Encourage the use of common and compatible tools sets for GEM and GND. Develop a common data strategy to enable GIG CS/IDM and set in place processes and procedures to affect GIG CM.

- **Objective 6.2:** Advocate Enterprise Management Capabilities and Solution(s) Congruent With Direction of Emerging DOD Policy and Guidance

Joint Staff Division Lead: J-6C

Move toward solutions for GIG EM that are compatible with other GIG systems and with DOD policy. Ensure that current joint programs (such as Joint Network Management System (JNMS)) support DOD policy and effective GEM. Support the NCOE tasks that attempt to bring together, under one program office, several of the major GIG

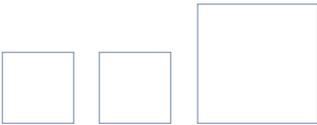
programs of record (including JTRS, Transformational Communications Satellite (TSAT), GIG Bandwidth Expansion and JNMS). Support ongoing GIG system engineering efforts to put into place the tool sets required to accomplish GEM.

- **Objective 6.3:** Promote Electromagnetic Spectrum Access and Awareness for DOD Forces Operating in Joint, Multinational, Interagency and Inter-Governmental Environments

Joint Staff Division Lead: J-6B

Obtaining access to the electromagnetic spectrum to support recent military operations has been impacted by issues such as securing host nation permission, spectrum access loss due to worldwide spectrum access reallocation, increased competition from commercial interests and the international frequency assignment process. Additionally, awareness of the electromagnetic spectrum—specifically of the requirements for gaining access to this vital resource—have long been an afterthought,





especially within the acquisition and operational communities. In order to support JNO, the joint community must advocate proper enforcement through adherence to national and international guidelines, protect current DOD electromagnetic spectrum allocations against encroachment and improve and develop electromagnetic spectrum policy. Focus must also shift to education and awareness throughout the operational and acquisition communities, in order to highlight the criticality of electromagnetic spectrum resources.

- **Objective 6.4:** Establish a Standardized Electromagnetic Spectrum Management Capability to Support DOD, Multinational, Interagency and Inter-Governmental Operations

Joint Staff Division Lead: J-6B

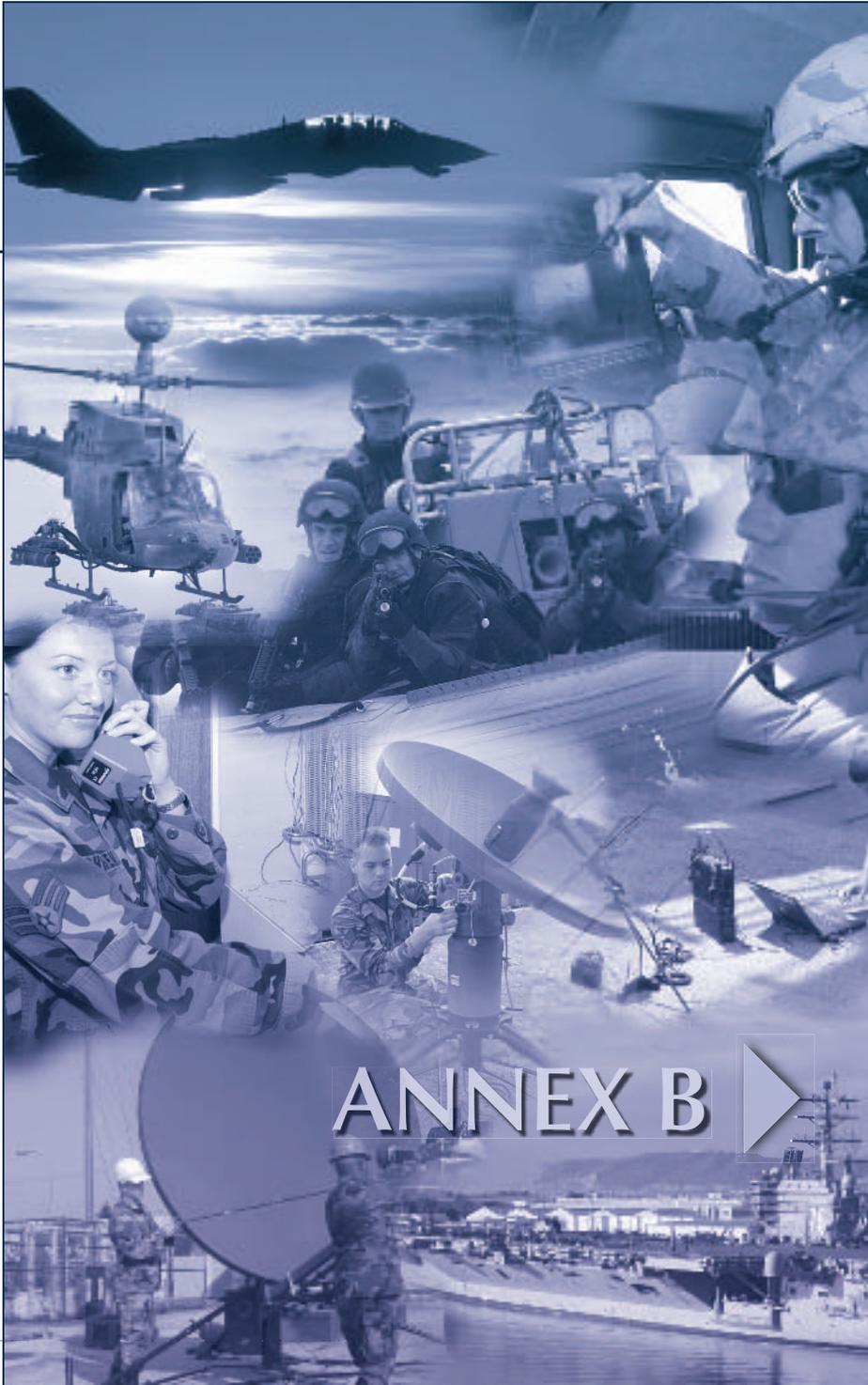
In the past, electromagnetic spectrum management within the United States and its possessions has been accomplished for the Department of Defense by the MILDEPs. Outside of the United States and its possessions, electromagnetic spectrum management has been accomplished by the geographic combatant commands. To accommodate the future roles and responsibilities of USNORTHCOM within the United States, as well as partnerships with multinational mission partners outside the United States and its possessions, the spectrum management process now needs to be re-evaluated. This re-evaluation includes advocating for the development of an overarching electromagnetic spectrum management tool suite to support joint

operations, including real-time and near-real-time detection, identification and update of a joint electromagnetic spectrum management database for all new emitters that support deconfliction and frequency assignments. Additionally, transformation within the electromagnetic spectrum management arena includes the development and acquisition of electromagnetic spectrum-dependent technology to support a continuously increasing electromagnetic spectrum demand.

- **Objective 6.5:** Develop a Cadre of Professional Electromagnetic Spectrum Management Personnel (Military and Civilian) Capable of Meeting the Demands Across the Continuum of Operations

Joint Staff Division Lead: J-6B

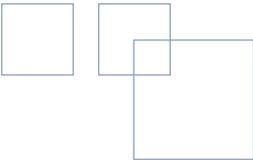
A cadre of qualified managers to fill joint electromagnetic spectrum management positions and to support electromagnetic spectrum management elements with multinational organizations and JTFs does not exist today. The Services need to establish and mature career field specialties in the spectrum management arena. Services must also establish efficient management processes for this undermanned, high demand career field. The maintenance of qualified electromagnetic spectrum career field personnel includes updating existing electromagnetic spectrum management training courses, tracking careers and assignments and defining wartime and peacetime proficiency requirements.



ANNEX B



- **Advanced Extremely High Frequency (AEHF)** – AEHF is the follow-on to Milstar and will be backward compatible with the Milstar waveforms. Currently scheduled to launch three satellites during FY08-10, AEHF provides up to ten times the capacity of Milstar—a significant increase in coverage—and the ability to support twice as many networks. It will support national, strategic and tactical users requiring protected, anti-jam, survivable communications for national crisis, Emergency Action Message dissemination, Integrated Tactical Warning/Attack Assessment, missile defense, presidential secure voice conferencing and interoperability with selected international partners.
- **Commercial SATCOM** – Commercial SATCOM provides much-needed augmented satellite support to deployed joint forces. Existing methods of forecasting and funding for these resources are usually ad hoc and cost prohibitive. In December 2004, the Department of Defense issued new policy as well as an action plan for planning, acquiring and managing commercial fixed satellite services. OSD, the joint community and DISA are working to create and implement a strategy that will improve the integration of commercial SATCOM services into the overall DOD architecture.
- **Deployable Joint Command and Control System (DJC2)** – DJC2 provides standing joint force headquarters (SJFHQs) and JFCs with a deployable, interoperable and scalable integrated C2 infrastructure supporting a common, standardized set of joint C2 capabilities, integrated applications, hardware, facilities and environmental control equipment. Residing at and deploying from either a combatant command headquarters or designated 2- or 3-star Service component headquarters, DJC2 will enhance a regional combatant commanders' ability to rapidly activate and deploy a JTF with a common package that sustains operations for days or weeks, supports efficient routing of distributed C2 through collaborative networks and decreases the lag between deployment and full operational capabilities. DJC2 includes limited external communications that can sustain only smaller or early stage joint force operations. Joint communications support element or organic Service-level assets shall provide enhanced or sustained communications requirements.



A maritime variant is planned for Increment II of the program.

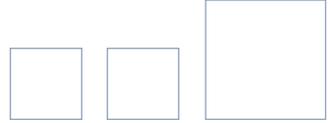
- **DOD CIO Executive Board** – The primary mission of this board is to advance DOD goals in the areas of information management, information interoperability and information security between and among Defense components. The board will coordinate with the IC CIO Executive Council on matters of mutual interest pertaining to the GIG. The board functions include management oversight; architecture management; interoperability, IA, or communications and computing infrastructure reviews; performance measures; acquisition process; resource allocation process; planning; waivers; and human resource management. The DOD CIO chairs the board. Members of the board include representatives from OSD, Service CIOs, Joint Staff/J-6, IC CIO, USJFCOM CIO, NSA, DISA and OSD Legal Counsel.
- **Enhanced Mobile Satellite Services (EMSS)** – EMSS is a commercially provided mobile satellite service supported by Iridium, LLC. Capabilities unique to EMSS include secure global handheld communications, E2E encryption (Type 1), protection of user information, high priority and special needs users and voice, data, messaging and paging services.
- **GIG Enterprise Services (GIG ES) and Net-Centric Enterprise Services (NCES)** – GIG ES and NCES are two DOD initiatives to transform the Department to a joint net-

centric environment. The GIG ES Initial Capabilities Document (ICD), approved by the JROC on 22 March 2004, describes “core” enterprise services available to all users and COI services available to all users within the particular COI.

The GIG ES aims to support an integrated, interoperable and networked joint force that will ensure common shared situation awareness, provide precise and actionable intelligence, support distributed and dispersed operations and ensure decision superiority enabling more agile and effective joint operations. GIG ES pertains to the joint force (both conventional and nuclear), intelligence and business domains and associated COI. This joint net-centric operating environment must support:

- Posting data to common, shared storage spaces as early as possible;
- Alerting decision makers to changes in relevant DOD, non-DOD and coalition information or time-critical events affecting their survival or threatening their mission;





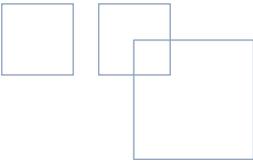
- Users and entities, down to the “first tactical mile,” with the capability to publish, subscribe and pull **what** they need **when** they want from **wherever** they are, limited only by the commander’s information management policy;
 - Defense-in-depth information assurance (IA) and security;
 - Pooling and sharing of information across multiple security domains;
 - Interoperability among interagency, inter-governmental and multinational partners;
 - The establishment of multiple position- or role-based profiles based on a users’ role, function and geographic location.
- Knowledge Capabilities
 - Collaboration
 - Application sharing
 - Session management
 - Discovery
 - Portal
 - Technical Capabilities
 - Enterprise content delivery network
 - Enterprise service management
 - Machine-to-machine messaging
 - Mediation
 - IA and security
 - Synchronization

GIG ES and NCES will provide DOD users the ability to use mission tailored information from anywhere within the network in a timely manner. This availability of information translates into a more effective and rapid execution of C2 within a given theater of operation and minimizes “forward deployed” systems in support of warfighting functions. GIG ES and NCES facilitate the transition from a platform-centric environment to a net-centric environment.

■ **GIG Information Assurance (GIG IA)** – IA capabilities and components that support the net-centric vision are a near-term DOD imperative. The IA objectives in support of the GIG architecture are:

- To develop common unifying approaches for DOD components and the IC.

The objective of NCES is to deliver a service-oriented infrastructure for timely and secure user access to DOD and other National Security information from anywhere. The NCES program will deliver “core” enterprise services upon which all other services will rely. The services include:



- To apply these approaches in the development and acquisition of systems incorporating IA and IA-enabled products and services

The essential element is that IA be an embedded feature, designed into every system, holistically, within the family of systems that comprise the GIG. This requires a shift from today's model consisting predominantly of link encryption and boundary protection between multiple discrete networks, to an E2E, seamless interconnected information environment using "Defense-in-Depth."

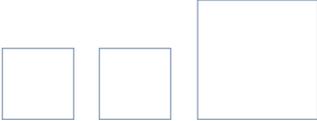
Given the magnitude of the GIG vision and its IA implications, the GIG will be realized through a phased implementation in order to ensure that the IA capabilities, guidance and policies exist to safely and deterministically evolve to the next GIG "spiral." This also allows for the GIG to incorporate new technologies as they emerge and drive the focus on targeted technology areas and associated standards development to realize the GIG vision capabilities.

- **Global Positioning System (GPS) III** – GPS currently provides highly accurate, real-time, all-weather, passive, common-reference grid position and time information to military and civilian users worldwide. The GPS III system will build on new capabilities being introduced by GPS IIR-M and Block IIF. Through this modernization program, the GPS Block II system adds two new civil signals on L2 and L5, adds a new exclusive military signal to L1 and L2 and adds flexible power to the Precise Positioning Service

on L1 and L2 for improved interference resistance. Scheduled for first launch in FY13, GPS III will provide increased power to military users for higher anti-jam capability, improved real-time accuracy, improved integrity and the ability to support prevention of adversary use of GPS.

- **Integrated Waveform (IW)** – IW is the latest waveform in Demand Assigned Multiple Access (DAMA) military standards. It will provide two to three times more capacity as legacy DAMA with improved voice quality and reduction in latency. IW can be applied to both 5kHz and 25kHz UHF SATCOM channels to meet increased warfighter demand for narrowband SATCOM.
- **Joint Tactical Radio System (JTRS)** – JTRS is an essential component to meeting 21st century warfighting requirements. It provides tactical units net-centric capabilities through connectivity to the GIG. JTRS is a software programmable radio that will provide real-time, voice, data and video communications among joint and coalition forces.

The JTRS is an IP-based radio set that includes routers, switches and other networking components and functions. It will transform today's single channel radio capability from a loosely integrated collection of legacy systems into an integrated E2E system of systems. The JTRS "Family of Radios" is interoperable with legacy communication systems and capable of adding new waveform requirements and technologies.



■ **Mobile User Objective System (MUOS)** – The MUOS will replace existing aging UFO satellite constellation. Four UHF satellites and one spare will be launched to provide on-demand, high capacity communications to support ISR and mobile weapon system platforms on the move in stressed environments. MUOS launches are currently scheduled for FY10-14.

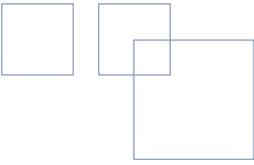


■ **Near Space** – (Emerging Capability) Near space platforms operating at altitudes between 65,000 and 325,000 feet may provide persistent, responsive and dedicated “space-like” capabilities to tactical and operational commanders. These systems, be they balloons, station-keeping airships, or unmanned aerial systems, exhibit potential for filling a revolutionary fourth layer of battlespace coverage to warfighters. Dependent on the payload, near space systems could provide commanders with communications, sensor and ISR capabilities that are currently unavailable due to high demand on available space platforms.

■ **Net Enabled Command Capability** – The NECC capability program will integrate existing and emerging C2 capabilities supporting the National Military Command System and JFCs through an enterprise-based, joint architecture-integrated application and database. This capability is targeted at the JTF commander in the Increment I capability that will be developed in the FY08-09 timeframe.

■ **Standing Joint Force Headquarters (SJFHQ)** – SJFHQ is a full-time, joint C2 element that is part of the regional combatant commander’s staff. The SJFHQ focuses on deliberate and crisis action planning and is a fully integrated participant in planning and operations activities. The SJFHQ exploits new organizational and operational concepts and technology to enhance the command’s peacetime planning efforts, accelerate the efficient formation of a JTF headquarters and facilitate crisis response by the joint force.

■ **Teleport** – A telecommunications collection and distribution point, providing deployed warfighters with worldwide access to multi-band, multimedia and worldwide reach-back capabilities through the DISN. Teleport is an extension of the Standardized Tactical Entry Point program, which currently provides reach-back for deployed warfighters via the Defense Satellite Communications System X-band satellites. This new system provides additional connectivity via multiple military and commercial SATCOM systems.

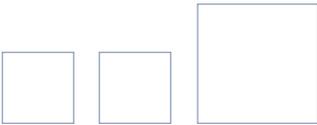


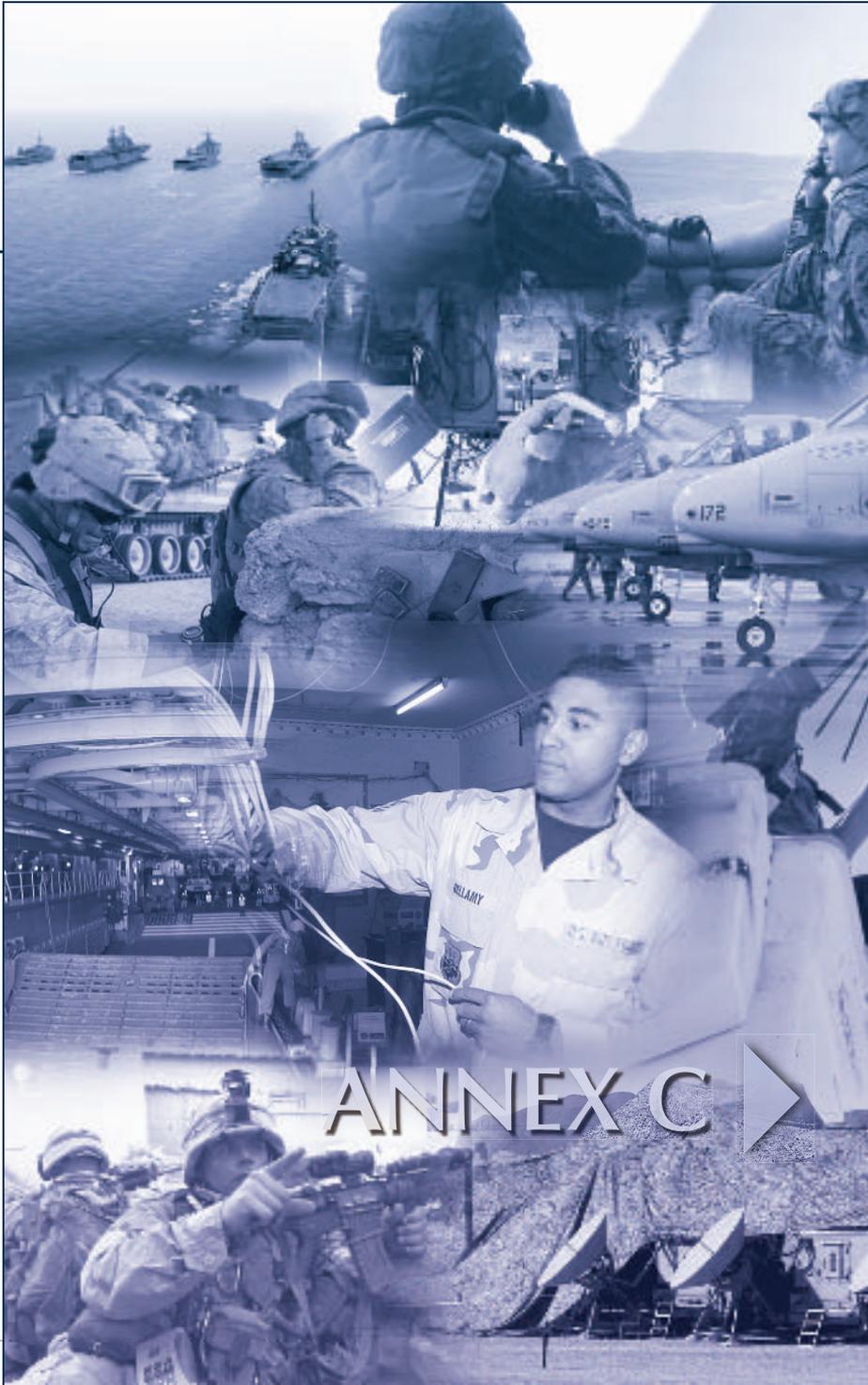
■ **Transformational Satellite Communications (TSAT)** – TSAT is the flagship satellite program for transformation to a net-centric warfighting capability and is an integral part of the transformational communications architecture. TSAT will consist of five laser cross-linked geosynchronous satellites, with the first launch in 2014 and full operational capability in 2018. TSAT will provide unprecedented connectivity with internet-like capability that extends the GIG to worldwide deployed and mobile users and will deliver a ten-fold increase in protected communications capacity over AEHF. TSAT will enable worldwide real-time connectivity to air and space ISR

■ **Wideband Gapfiller System (WGS)** – WGS provides unprotected satellite bandwidth primarily for deployed forces and warfighter communications. It will replace the aging Defense Satellite Communication System and Global Broadcast Service satellites, providing the Department of Defense with high-capacity, wideband service for the Nation. WGS embodies key SATCOM evolutions, providing increased bandwidth efficiency and flexibility to route communications between many users in a variety of settings. This program consists of five satellites. The first three are planned for launch from FY07-08.



assets, providing increased situational awareness and targeting information to the warfighter. TSAT will provide protected tactical communications-on-the-move necessary to achieve direct and interoperable net-centric warfighting and situational awareness.

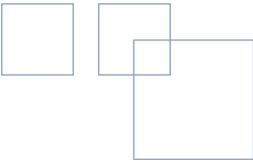




ANNEX C



- **The Defense Acquisition System (DODD 5000.1 and DODI 5000.2).** The Defense Acquisition System is the management process by which the DOD provides effective, affordable and timely systems to the users. It exists to manage the Nation's investments in technologies, programs and product support necessary to achieve the National Security Strategy and support the United States Armed Forces.
- **Planning, Programming, Budget and Execution (PPBE) (DODD 7045.14/MID-913).** The PPBE process is the DOD resource allocation process controlled by the Secretary of Defense. PPBE is used to establish, maintain and revise the Future Years Defense Plan (FYDP) and execute the DOD portion of the President's budget.
- **Joint Capabilities Integration and Development System (JCIDS) (CJCSI 3170.01).** The procedures established in the JCIDS support the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council (JROC) in identifying, assessing and prioritizing joint military capability needs. JCIDS implements a capabilities-based approach that better leverages the expertise of all government agencies, industry and academia to identify improvements to existing capabilities and to develop new warfighting capabilities. This approach requires a collaborative process that utilizes joint concepts and integrated architectures to identify prioritized capability gaps and synchronizes DOTMLPF solutions (materiel and nonmateriel) to resolve those gaps.
 - FCBs are intended to lead the review of Service-proposed functional needs analysis to ensure compliance with the series of JCIDS documents and to make recommendations to the Joint Capabilities Board (JCB) and the JROC.
 - **Net-Centric Functional Capabilities Board (NC FCB).** The NC FCB is responsible for the organization, analysis and prioritization of joint warfighting capability needs within the assigned joint net-centric operations functional area. The NC FCB has four primary responsibilities:



- Oversee a portfolio of net-centric capabilities within JCIDS; the acquisition process; and the PPBE process.
- Lead development of net-centric-related concepts, operational views of integrated architectures and related studies. Net-Centric FCB will use these products as the framework to perform net-centric capability analyses in support of JCIDS.
- Ensure horizontal integration of net-centric capabilities across the other FCB functional areas.
- Ensure vertical and horizontal integration of communications capabilities across national, strategic, operational and tactical levels.

The NC FCB functions include:

- Oversee the development and maintenance of net-centric-related functional and integrating concepts and integrated architectures for JROC approval. These net-centric concepts will include capabilities, attributes, measures and metrics.
- Coordination, integration and deconfliction of capability proposals affecting the net-centric portfolio.
- Developing a net-centric conceptual framework, including capabilities, attributes, measures and metrics that apply to all other

functional areas. Also, it must enforce net-centric standards (e.g. the Net-Ready Key Performance Parameter, the Net-Centric Data Strategy and the Net-Centric Operations and Warfare Reference Model) that cut across all of the FCBs. The NC FCB shall provide representatives to the other FCBs to conduct reviews and make recommendations on programs and issues with net-centric implications.

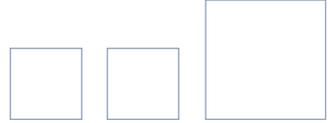
- Evaluating JCIDS documents for applicability within the Net-Centric FCB portfolio. The Net-Centric FCB will provide recommendations to the JROC via the JCB.

□ Senior Warfighter Forum (SWaF).

The SWaF is a JROC-directed forum used to organize, analyze, prioritize and frame complex warfighting resources and requirements issues for JROC approval. A JROC tasking memorandum will identify the scope, sponsor and supporting agencies to frame the issues. The SWaF is a tool for combatant commanders to use to identify a joint requirements issue or resource mismatch.

■ Military Communications-Electronic Board (MCEB).

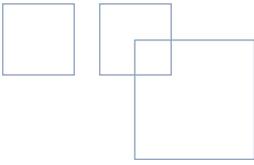
The MCEB shall consider those military communications-electronics issues referred by the Secretary of Defense, Chairman of the Joint Chiefs of Staff, DOD CIO, MILDEPs and head of other DOD Components. The Joint Staff/J-6 chairs the MCEB. Membership of the board is composed of representatives



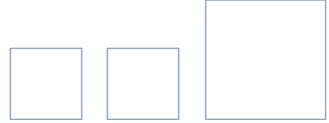
from each Service, US Coast Guard, DISA, Defense Intelligence Agency, NSA and the Vice-Director of J-6, who represents the combatant commanders. ASD(NII) is the only non-chartered member invited to attend the executive session. The MCEB is the senior resolution, coordination and prioritization body for matters related to NSS communications and interoperability testing issues within the warfighting enterprise mission area. The MCEB Chair will inform the DOD CIO of all MCEB related matters that may have an impact on DOD CIO responsibilities.

ANNEX D: ACRONYMS

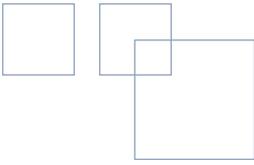
#QFY##	# Quarter, Fiscal Year ##
AEHF	Advanced Extremely High Frequency
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)
C2	Command and Control
C2IP	Command and Control Initiative Program
C/S/A	Combatant Command, Service and Agency
CBA	Capability-Based Assessment
CDD	Capability Development Document
CDMO	Cross-Domain Management Office
CDS	Cross-Domain Solution
CES	Core Enterprise Services
CFBLNet	Combined Federated Battle Laboratories Network
CIIT	Capabilities Improvement Initiative Team
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CM	Configuration Management
CND	Computer Network Defense
COI	Community of Interest
COMOPTEVFOR	Commander, Operational Test and Evaluation Force
COMSEC	Communications Security
CONOPS	Concept of Operations
COP	Common Operational Picture



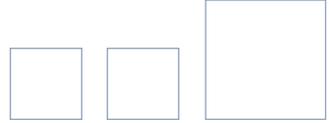
COTP	Common Operational and Tactical Pictures	DOTMLPF	Doctrine, Organization, Training, Material, Leadership and Education, Personnel and Facilities
CPD	Capabilities Product Document	DREN	Defense Research and Engineering Network
CS	Content Staging	E2E	End-to-End
CWID	Coalition Warrior Interoperability Demonstration	EMI	Electro-Magnetic Interference
DAMA	Demand Assigned Multiple Access	EMSS	Enhanced Mobile Satellite Services
DAS	Defense Acquisition System	ERM	Execution Roadmap
DAWG	Deputy's Advisory Working Group	ES	Enterprise Services
DISA	Defense Information Systems Agency	ESSG	Enterprise Solution Steering Group
DISN	Defense Information Systems Network	FCB	Functional Capabilities Board
DISN-LES	Defense Information Systems Network – Leading Edge Services	FJAWG	Functional Joint Architecture Working Group
DISR	DOD Information Technology Standards Registry	G/FO	General/Flag Officer
DJC2	Deployable Joint Command and Control	GCCS-J	Global Command and Control System–Joint
DMS	Defense Message System	GEM	GIG Enterprise Management
DNI	Director of National Intelligence	GIAP	GIG Information Assurance Portfolio
DOD	Department of Defense	GIG	Global Information Grid
DODD	Department of Defense Directive	GND	GIG Network Defense
DODI	Department of Defense Instruction	GPS	Global Positioning System
DOT&E	Director of Operational Test and Evaluation (OSD)	GRIFFIN	Globally Reaching Interactive Fully Functional Information Network
		GWOT	Global War on Terrorism



HAIPE	High Assurance Internet Protocol Encryptor	JIC	Joint Integrating Concept
I&S	Interoperability and Supportability	JMETC	Joint Mission Environment Test Capability
IA	Information Assurance	JNMS	Joint Network Management System
IC	Intelligence Community	JNO	Joint Net-Centric Operations
ICD	Initial Capabilities Document	JOC	Joint Operating Concept
IDM	Information Dissemination Management	JP	Joint Publication
IP	Internet Protocol	JROC	Joint Requirements Oversight Council
IPL	Integrated Priority List	JTF	Joint Task Force
IPv6	Internet Protocol Version 6	JTF-GNO	Joint Task Force – Global Network Operations
ISP	Information Support Plans	JTRS	Joint Tactical Radio System
ISR	Intelligence, Surveillance and Reconnaissance	JUON	Joint Urgent Operational Need
IT	Information Technology	KIP	Key Interface Profile
IW	Integrated Waveform	KM	Knowledge Management
J-6	Command, Control, Communications and Computer Systems Directorate, Joint Staff	M&S	Modeling and Simulation
JBMC2	Joint Battle Management Command and Control	MCEB	Military Communications-Electronics Board
JCA	Joint Capability Area	MCO	Major Combat Operations
JCB	Joint Capabilities Board	MDA	Milestone Decision Authority
JCD	Joint Capabilities Document	MILDEP	Military Department
JCIDS	Joint Capabilities Integration and Development System	MNIS	Multinational Information Sharing
JCW	Joint Community Warfighter	MOA	Memorandum of Agreement
JFC	Joint Force Commander	MOE	Measures of Effectiveness
		MUOS	Mobile User Objective System



NATO	North Atlantic Treaty Organization	POM	Program Objective Memorandum
NC FCB	Net-Centric Functional Capabilities Board	POR	Program of Record
NCDS	Net-Centric Data Strategy	PPBE	Planning, Programming, Budgeting and Execution
NCE	Net-Centric Environment	QDR	Quadrennial Defense Review
NCES	Net-Centric Enterprise Services	SA	Situational Awareness
NCID	Net-Centric Implementation Directive	SATCOM	Satellite Communications
NCOE	Net-Centric Operational Environment	SDB	SATCOM Database
NECC	Net-Enabled Command Capability	SE	Systems Engineering
NetOps	Network Operations	SecDef	Secretary of Defense
NETWARS	Network Warfare Simulation	SIPRNET	Secret Internet Protocol Router Network
NIPRNET	Non-Secure Internet Protocol Router Network	SJFHQ	Standing Joint Force Headquarters
NM	Network Management	SPG	Strategic Planning Guidance
NMS	National Military Strategy	SWarF	Senior Warfighter Forum
NMS-CO	National Military Strategy for Cyberspace Operations	TD	Technology Development
NSA	National Security Agency	TJE	Testing in the Joint Environment
NSS	National Security Systems	TOR	Terms of Reference
OODA	Observe, Orient, Decide, Act	TSAT	Transformational Satellite Communications
OPR	Office of Primary Responsibility	TTP	Tactics, Techniques and Procedures
PfM	Portfolio Management	UHF	Ultra-High Frequency
POA&M	Plan of Action and Milestones	USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
		USD(I)	Under Secretary of Defense for Intelligence
		USEUCOM	United States European Command



USJFCOM	United States Joint Forces Command
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSTRATCOM	United States Strategic Command
WGS	Wideband Gapfiller System
WMA	Warfighting Mission Area

ANNEX D: DEFINITIONS

application — A locally resident software program or group of programs that interfaces directly with joint force decision makers and communities of interest and carries out generalized or mission-specific tasks or processes for which a computer is used, i.e., word processing, spreadsheets, graphics, database management and communications packages.

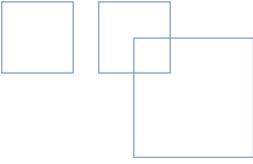
battlespace — The environment, factors and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea and space of enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest.

capability — The ability to execute a specified course of action. (A capability may or may not be accompanied by an intention.)

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

command and control system — The facilities, equipment, communications, procedures and personnel essential to a commander for planning, directing and controlling operations of assigned and attached forces pursuant to the missions assigned. *(JP 1-02)*

communities of interest — An inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. **Also called COI.** *(DOD Net-Centric Data Strategy)*



computer network defense — Actions taken to protect monitor, analyze, detect and respond to unauthorized access within DOD information systems and computer networks. Also called CND. (JP 1-02)

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

control — Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. (JP 1-02)

critical infrastructure protection — The identification, assessment and assurance of cyber and physical mission-critical capabilities and requirements, to include the political, economic, technological and information security environments essential to the execution of the NMS. It encompasses the infrastructure necessary for deterrence operations and that is essential to plan, mobilize, deploy and sustain military operations and transition to post conflict operations. Involved infrastructures may be DOD-owned or belong to other US government agencies, commercial, or private sector entities. Additionally, infrastructure may be owned and controlled by foreign commercial, private sector and/or host nation organizations and governments. Also called CIP. (Proposed for inclusion in JP 1-02)

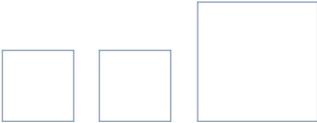
cyberspace — A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures. (Proposed for inclusion in JP 1-02)

enterprise services — The ability to provide well-defined, enterprise network functions that accept a request and return a response through an interface with a user or another service such as collaboration, messaging, or information discovery and storage. (Derived from NCOE JIC)

“first tactical mile” — The support that the net-centric environment will provide to warfighters directly involved in executing the mission and warfighters at the “edge” of the network.

Global Command and Control System — A deployable command and control system supporting forces for joint and multinational operations across the range of military operations with compatible, interoperable and integrated communications systems. Also called GCCS. (JP 1-02)

Global Information Grid — The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel. The Global Information Grid (GIG) includes all owned and leased communications and computing systems and services, software (including



applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, National Security and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied and non-DOD users and systems. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria: (1) Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software and services. (2) Provides retention, organization, visualization, IA, or disposition of data, information and/or knowledge received from or transmitted to other equipment, software and services. (3) Processes data or information for use by other equipment, software and services. Non-GIG information technology (IT) is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. **Also called GIG.** (JP 1-02)

information —

1. Facts, data, or instructions in any medium or form.

2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

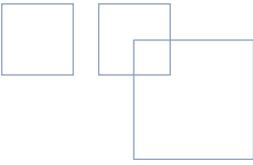
information assurance — Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities. **Also called IA.** (JP 1-02)

information environment — The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (JP 1-02)

information management — The planning, budgeting, manipulating and controlling of information throughout its life cycle. (JP 1-02)

information superiority — The operational advantage derived from the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Approved for inclusion in the next version of JP 1-02 through approval of JP 3-13.)

information transport — The ability to provide the physical communications media over which assured connectivity takes place, supported by switching and routing systems and the computing infrastructure. (Derived from NCE Joint Functional Concept)



interoperability —

1. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.
2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (JP 1-02)

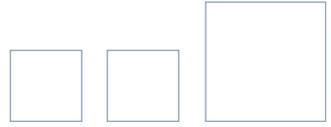
knowledge management — The ability to systematically discover, select, organize, distill, share, develop and use information in a social domain context to improve warfighter effectiveness. Also called KM. (Derived from NCOE JIC)

network management (within a joint task force) — The process of planning, engineering, activating, monitoring, controlling and adjusting the performance of the joint task force (JTF) backbone network, common user systems within the joint operational area and interfaces to other systems and networks, to include those functions associated with operating the network; i.e., spectrum management, security management and information operations. (CJCSM 6231.07C)

network operations — The organizations and procedures required to monitor, manage and control the Global Information Grid. Network operations incorporate network management, information dissemination management and information assurance. Also called NetOps. (JP 1-02)

SECRET Internet Protocol Router Network — The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called SIPRNET. (JP 1-02)

standardization — The process by which the Department of Defense achieves the closest practicable cooperation among the Services and Defense agencies for the most efficient use of research, development and production resources and agrees to adopt on the broadest possible basis the use of: a. common or compatible operational, administrative and logistic procedures; b. common or compatible technical procedures and criteria; c. common, compatible, or interchangeable supplies, components, weapons, or equipment; and, d. common or compatible tactical doctrine with corresponding organizational compatibility. (JP 1-02)



ANNEX E: REFERENCES

Department of Defense, *National Defense Strategy of the United States of America*, March 2005.

Department of Defense, *Quadrennial Defense Review Report*, 6 February 2006.

DOD CIO, *DoD CIO Annual Report – Working Draft*, 10 January 2006.

DOD CIO, *GIG Core Services Coordination Decision Paper – Coordination Review Draft*, 21 December 2005.

Chairman of the Joint Chiefs of Staff, *Synopsis – The 16th Chairman’s Guidance to the Joint Staff*, 1 October 2005.

Chairman of the Joint Chiefs of Staff, *Quadrennial Defense Review Report, Chairman’s Assessment of the 2006 Quadrennial Defense Review*, 6 February 2006.

Joint Staff, *Capstone Concept for Joint Operations, Version 2.0*, August 2005.

Joint Staff, *Major Combat Operations Joint Operating Concept*, September 2004.

Joint Staff, *Net-Centric Operational Environment Joint Integrating Concept*, 31 October 2005.

Joint Staff, *Net-Centric Operational Environment (NCOE) Roadmap-Draft*, 23 January 2006.

USSTRATCOM, *Joint Concept of Operations for Global Information Grid NetOps*, 15 August 2005.

US Pacific Command, *NETOPS Background... Joint Commanders Challenge*, Presentation Slide, n.d.



Point of Contact:

J-6 Director's Action Group
DSN 671-0186 or 671-9885
703-571-0186 or 703-571-9885

<http://www.jcs.mil/j6/jointcampaign.html>