Department of Defense
NetOps Strategic Vision

December 2008

Department of Defense
Chief Information Officer
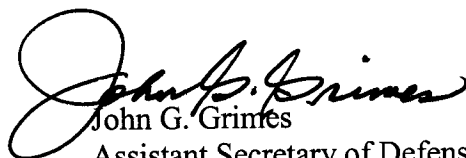## The Pentagon – Washington, D.C.

Foreword

The Department of Defense (DoD) is transforming its military to a net-enabled, agile force that can deal with uncertain and changing environments. We are pursuing effective Net-Centric Operations, in part, by evolving the Department's Global Information Grid (GIG) to facilitate widespread sharing of trusted information and rapid adaptation of forces to changing mission needs. The GIG will provide a supportive information environment wherein every user can obtain the information needed when and where it is needed, even in unanticipated situations. A key to fully achieving this potential is a robust set of DoD-wide NetOps capabilities: the operational, organizational, and technical capabilities for operating and defending the GIG. NetOps will make the GIG a more effective weapon to meet changing mission needs and to support operations in the cyberspace domain. NetOps will provide efficient and dynamic allocation of GIG resources and protect the GIG's information environment to enable trust in its use and in the information it contains.

Achieving our vision of a dynamic, visible, and managed network environment will be a challenge. It will require major improvements in shared GIG situational awareness and significant changes in the overarching approach for GIG command and control (C2). But the rewards are great, since our envisioned NetOps capability will provide GIG users, particularly those on the tactical edge, timely information to effectively and efficiently apply all GIG resources in support of multi-mission demands.

This NetOps Strategic Vision builds on the underlying tenets of net-centricity and other Net-Centric strategies. It outlines a vision that transforms NetOps capabilities into a force multiplier by enabling warfighters, business and intelligence users and decision makers to fully employ the power of the GIG. This Strategic Vision seeks to establish a Net-Centric NetOps capability for dynamically operating and defending the GIG as a unified, agile enterprise that provides responsive support to multiple simultaneous missions. This new unified NetOps capability is based on these goals:

- Share GIG Situational Awareness,
- Unify GIG Command and Control, and
- Institutionalize NetOps.

Realizing this vision will require a cohesive effort by the entire NetOps community and the customers they support.

John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Table of Contents

List of Figures

List of Tables

1   Purpose

The purpose of the NetOps Strategic Vision is to communicate the DoD CIO's vision and goals for migrating to new NetOps capabilities which will enable the Department's Net-Centric vision.   It builds on the DoD Information Management/Information Technology (IM/IT) Strategic Plan, the GIG Architectural Vision, and supporting Net-Centric strategies.   This document is intended to do the following: guide the Department's NetOps activities, initiatives, and investments; foster unity of effort throughout DoD and its mission partners; serve as a framework for governing the evolution of NetOps capabilities; and provide the foundation for planning the coherent implementation of NetOps across the DoD.

The NetOps Strategic Vision is written for Department leadership including the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, and Agencies. It provides insight for the Department's mission partners and other organizations engaged in the operation and defense of the GIG. Commanders, warfighters, system and service developers, and acquisition personnel must understand the vision for NetOps.   Areas of responsibility for this new construct have been defined in Departmental policy and guidance such as the Defense Information Enterprise Architecture version 1.0 and will be formalized in the DoD Instruction, *NetOps for the GIG*.

2   Introduction

2.1   NetOps Overview

As the globally interconnected set of DoD information capabilities, the GIG is truly a set of Joint capabilities that are used throughout DoD. The information and functional capabilities it provides impact every aspect of DoD operations.

> The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, 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.[1]

NetOps is defined as the DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG.   NetOps includes, but is not limited to, enterprise management, net assurance[2], and content management.   NetOps provides commanders with GIG situational awareness to make informed command and control decisions. GIG situational awareness is gained through the operational and technical integration of enterprise

---

[1] DoD Directive 8100.1, September 19, 2002
[2] This term formerly referred to as "Net Defense"

management and defense actions and activities across all levels of command (strategic, operational, and tactical). [3]

- Enterprise Management is the set of functional capabilities and operational processes necessary to monitor, manage, and control the availability, allocation, and performance within and across the GIG. It includes Enterprise Services Management, Applications Management, Computing Infrastructure Management, Network Management, Satellite Communications Management, and Electromagnetic Spectrum Management.

- Net Assurance is the set of functional capabilities and operational processes necessary to protect and defend the GIG. This includes the operational responsibilities for information assurance, computer network defense (to include Computer Network Defense Response Actions), and critical infrastructure protection in defense of the GIG.

- Content Management is the set of functional capabilities and operational processes necessary to manage, and facilitate the visibility and accessibility of information within and across the GIG.

NetOps influences all core segments of the GIG and associated capabilities in the Net-Centric capability portfolio[4] which encompasses Net Management as well as those associated with Information Transport, Enterprise Services and Information Assurance. By linking these operational, technical and programmatic perspectives to achieve integrated capabilities, NetOps assures the availability, protection and integrity of DoD networks, systems, services, and information.

In support of NetOps, the United States Strategic Command (USSTRATCOM) is responsible for planning, integrating, and coordinating DoD's global network operations by directing GIG operations and defense and by advocating the respective desired characteristics and capabilities. USSTRATCOM executes this mission through the Joint Task Force–Global Network Operations (JTF-GNO) with the full and active participation by the entire joint community. Every DoD Component and partner organization that develops, deploys, operates, or uses any portion of the GIG plays a role in the accomplishment of this mission from the Combatant Commands and Services through acquisition executives and materiel developers who must ensure capabilities destined for use as part of the GIG are supportive of NetOps and USSTRATCOM's role.

2.2   The Role of NetOps in Net-Centric Operations

The role of NetOps in Net-Centric Operations is to enable the GIG to provide users at all levels and in all operational environments access to and use of the information they need. As depicted in Figure 1, NetOps is a critical operational enabler, and forms the core of GIG operations in a Net-Centric framework. NetOps enables the operations and defense within and across GIG information transport, enterprise services, and information assurance capabilities.

---

[3] DoD Instruction, NetOps for the GIG, Draft Final, July 2008
[4] Net-Centric Joint Capability Area (JCA) Tier 2

It does so in a way that creates a trusted environment capable of protecting and maintaining the integrity, quality, and availability of information. This trusted environment enables users to post, access, and share relevant information and to collaborate on the development and/or use of such information. This environment also enables forces to conduct Net-Centric Operations and superior decision making through shared understanding, and agile force synchronization.
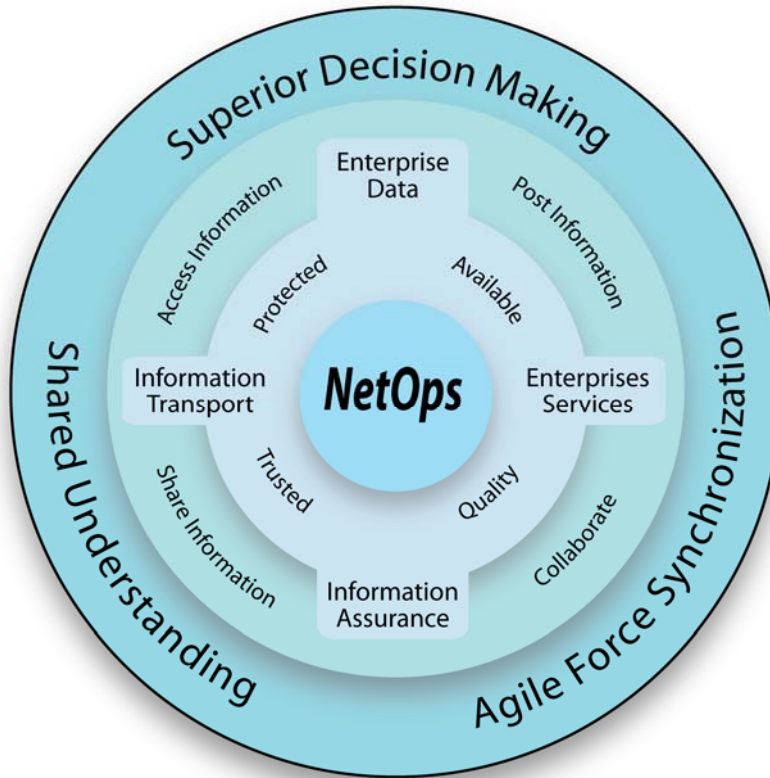
Figure 1.   NetOps Enabled Net-Centric Operations

2.3   NetOps Today

NetOps has yet to transcend the organizational and functional stovepipes of individual GIG networks in terms of interoperability and information access.   While each of these stovepipes has its own management capability, DoD does not yet share information to manage across domains. The result is relatively static configurations that limit NetOps and GIG agility in the face of rapidly changing and

Providing a robust, DoD-wide NetOps capability would significantly enhance the ability of the operators/defenders of the GIG to fully support warfighting and non-warfighting missions in an increasingly joint and multi-partner environment.

unanticipated mission needs. The Joint NetOps Concept of Operations[5] has enabled the DoD to begin significantly improving how the GIG is operated and defended. Also the Net-Centric Functional Capability Board within the Joint Capabilities Integration and Development System (JCIDS) process and the related Net-Centric Capability Portfolio Manager (NC CPM) initiative[6] have begun to address many of the key deficiencies that have been reported from operation Iraqi Freedom and day-to-day operations. Continued organizational, technological and process changes will enable a significantly more unified, timely and responsive GIG NetOps that can fully enable net-centric operations by providing:

- Timely and complete GIG Situational Awareness information to Commanders

- GIG Command and Control capabilities that enable rapid decision making

- Clear, well integrated and enforceable NetOps operational policies

- More effective, coordinated operational use of the electromagnetic spectrum

- Standardized metrics that enable the measurement of the health and mission readiness across the GIG

- Automated, federated NetOps capabilities that enable the rapid adaption of GIG capabilities to rapidly changing mission needs and unanticipated threats.

- Increased coordination, alignment and synchronization of NetOps acquisition and fielding activities currently under way

Addressing these capabilities will significantly improve the ability of the operators and defenders of the GIG to fully support ongoing warfighting and peacekeeping missions in an increasingly joint and multi-partner environment. However, there is a need for overarching operationally based guidance to ensure unity of effort in transforming NetOps to this end.

3 NetOps in the Future

3.1 The NetOps Challenge

To provide the capabilities outlined in the previous section, NetOps will transform along with the GIG, to dynamically support new warfighting, intelligence, and business processes and enable users to access and share trusted information in a timely manner. The future GIG will result in a richer Net-Centric information environment comprised of shared services and capabilities based on advanced technologies. It will be heavily reliant on end-to-end virtual networks to interconnect anyone, anywhere, at

> The overarching NetOps challenge is to be able to operate and defend the GIG as a single, unified, agile and adaptive enterprise capable of providing responsive and resilient support to multiple simultaneous mission areas under uncertain and changing conditions.

---

[5] Joint Concept of Operations for GIG NetOps, Version3, 4 August 2006
[6] Network Management & Spectrum Management Functional Solutions Analysis (NM & SP FSA); Final Draft, 16 May 2008

any time with any type of information through voice, video, images, or text. It will also be faced with even greater security threats that NetOps must help address.

In a Net-Centric environment, the core GIG capabilities (e.g. Information transport, Enterprise Services, and Information Assurance) and the applications they support will become increasingly dynamic with new capabilities being deployed, configured, re-configured, and removed as needed to meet the needs of an agile force and dynamic mission requirements. This new and dynamic environment will require that NetOps be executed in an equally dynamic way.

As the current Base Realignment and Closure progresses, Commanders and staff elements will find themselves increasingly operating in an environment that they do not directly control. For example, an Air Force or Army unit may be Joint-based on each other's installation, which will require them to use the host organization's networked infrastructure and conform to the host's policies. Another example would be if a user at a Navy or Marine Corps installation had to access Army services, information, or data to do operational planning. While there are some notable exceptions, this is in sharp contrast to today's environment, in which most services and capabilities are Service stovepipes owned and controlled by individual units or organizations. In a shared environment, warfighters will have to trust that services and capabilities will be available when and where they are needed.

NetOps requires dynamic, flexible, integrated management capabilities that enable rapid synchronization of decisions at appropriate levels across different areas of responsibility or domains within the GIG. This will facilitate the decision-making necessary to quickly identify problems, shift resources, change configurations and coordinate management of the GIG infrastructure and capabilities.

Finally, the future NetOps must provide Commanders with the ability to effectively control, manage, defend, and operate in and through the cyberspace domain. The National Military Strategy for Cyberspace Operations lays the initial groundwork for this effort and NetOps must continue to evolve and support this integral component of future warfighting.

3.2 The Vision for Net-Centric NetOps

To meet the NetOps challenge, a fundamentally improved approach for performing NetOps is necessary – one that involves major improvements in the ability to achieve GIG shared situational awareness and significant changes in the overarching approach to C2 of the GIG as well as the enabling capabilities; the way these capabilities are provided across DoD, and most importantly the way they are viewed and employed by the GIG's users. The vision is to transform existing and new NetOps capabilities into a force multiplier that enables the warfighters, business, and intelligence users and decision makers to fully employ the

> The NetOps Vision is to transform existing and new NetOps capabilities into a force multiplier that enables warfighter, business, intelligence, and enterprise information environment users and decision makers to fully employ the power of the GIG.

power of the GIG. This vision will be attained by establishing NetOps capabilities that are:

- Mission Oriented: All information dependent processes necessary for a mission can be effectively supported;

- User Focused: Users can access and obtain needed information from anywhere in the GIG in a timely manner; even when their needs are unanticipated;

- Globally Agile: Rapidly changing and unanticipated mission priorities and requirements can be met by dynamically maneuvering GIG resources; and

- Institutionally Transformed: NetOps capabilities evolve smoothly in concert with GIG capabilities and emerging Net-Centric operational concepts.

This vision will require developing and implementing agile and responsive planning, engineering and provisioning capabilities. In this vision, GIG situational awareness information will be shared with GIG authorized users so they can collaborate on meeting mission needs or assessing the impact of GIG changes on mission accomplishment. NetOps personnel will use shared situational awareness to proactively manage the GIG to meet commander's intent and to rapidly respond to unexpected changes in threats and mission needs. Shared situational awareness will facilitate central oversight of critical GIG assets and rapid integrated management and execution of decisions. This will be accomplished through decentralized policy-based management with a high degree of automated support and by employing consistent tactics, techniques, and procedures that enable the conduct of coherent operations in a federated GIG environment.

In the future, NetOps will be able to routinely, rapidly, and accurately reallocate or reconfigure GIG resources, including elements such as information assurance devices, computing processing and storage capacities, and network throughputs to meet changing mission needs and threats. All NetOps tasks necessary to enable data access, information flow, and user collaboration across management boundaries or domains will be synchronized and executed at an appropriate level of detail. Commanders will be able to understand the state of the GIG as it relates to their missions and the associated tradeoffs in performance, security, and agility that could impact the mission. Warfighters and other users will be confident that the GIG can be tailored to meet their needs and can be leveraged to enhance the agility and effectiveness of their forces.

NetOps capabilities will be developed, implemented, and matured as time-phased capability increments. These defined capability increments will be consistent with and supportive of the DoD's evolving Net-Centric operational concepts. Transforming and maturing NetOps will involve work in many non-technical areas that span Doctrine, Organization, Training, Material, Leadership and Education, Personnel and Facilities (DOTMLPF). A critical aspect of NetOps transformation will be the creation of policy, governance structures, implementation plans, and metrics that will be necessary to guide NetOps evolution.

4 The Net-Centric NetOps Strategic Vision Goals and Objectives

The following sections describe a set of goals and objectives that are intended to serve as actionable guidance for achieving the NetOps Vision. The goals described in Table 1 are focused on achieving operational outcomes, not on developing and deploying specific technical implementations. This recognizes that the major hurdles associated with transforming NetOps are organizational, procedural, or cultural in nature. While there are also technical challenges, the Department must first and foremost fundamentally re-think how it conducts NetOps in order for the GIG to be truly responsive to mission needs and to effectively support operations in cyberspace. Each goal identifies high-priority objectives for meeting that goal.

Table 1. Goals for Net-Centric NetOps

Goals	Description
Share GIG Situational Awareness	Provide GIG users, operators, and commanders at all levels with accurate and timely information that enables a shared understanding of the health and mission readiness of the GIG.
Unify GIG Command and Control	Adopt a unified C2 approach for agile proactive management of the GIG.
Institutionalize NetOps	Institutionalize NetOps across DOTMLPF to ensure DoD requirements, acquisition, budgeting, and management processes can be influenced to achieve the NetOps vision.

4.1 Goal 1: Share GIG Situational Awareness

Provide GIG users, operators, and commanders at all levels with accurate and timely information that enables a shared understanding of the health and mission readiness of the GIG.

4.1.1 Objective: Make NetOps data visible, accessible, and understandable to all authorized users

Effective and efficient management of the GIG requires accurate, timely, and relevant situational awareness. Authorized users must be able to quickly find, access, retrieve, and analyze information related to the operational health, performance, security, and mission readiness of the GIG. Achieving this objective will require the adoption of Department-wide, industry based standards for posting and sharing NetOps information. This will ensure that authorized users, to include mission partners, will have access to the NetOps information they need to support operational missions. NetOps must move from a point-to-point information sharing model to one that exposes NetOps data and information to any authorized user (person or machine) using agreed-upon data models and mechanisms.

Owners and managers of NetOps capabilities must comply with the DoD Net-Centric Data Strategy by making all NetOps data visible, accessible, and understandable to all authorized users. This is necessary to support critical processes among NetOps centers; such as processes for fault identification, isolation, and correction, as well as those for information assurance and computer network defense activities. Adopting industry based standards will also improve the Department's ability to share NetOps information with mission partners and commercial entities that support and provide information technology services and capabilities to the DoD. NetOps personnel and the users they support must be able to access NetOps data commensurate with its operational and security sensitivity and their assigned and authorized permissions. This means that it will be necessary to develop rules to govern access to NetOps data. NetOps data must also be made available in ways that support users equipped with different access mechanisms, (e.g. desktop or laptop versus personal digital assistants, etc.).

Finally it is no longer possible to predict in advance all who might need access to NetOps information; therefore NetOps information sharing approaches must be able to accommodate the unanticipated or ad hoc user. For instance, a Combatant Command J4, who traditionally might not be considered a user of NetOps information, may want to know the reliability of a service that was not specifically developed for his mission. He might want to understand whether a Defense Logistics Agency service that provides order confirmation and availability status to wholesale logistics centers is reliable (i.e., operational all the time, endorsed by the people who rely on it, etc.).

4.1.2   Objective: Provide GIG Situational Awareness information in a mission context

Commanders at all levels must be provided with the understanding of how events happening across the GIG impact their operations. NetOps personnel must make information related to the health and mission readiness of the GIG available to Commanders in a form that can be easily adapted to their mission context. Rather than simply informing a Commander that a network router is "down" or that a critical battlefield application service that operates over a satellite link is experiencing excessive delay, NetOps must have the ability to report an event in terms of what it means to mission success.

4.1.3   Objective: Establish metrics for measuring the health and mission readiness of the GIG

DoD must develop NetOps metrics and measures from two perspectives. The first reflects the need for common metrics to characterize the health of the GIG in terms of operational status, performance, and vulnerability. The second is from a mission readiness perspective, which captures and details how well the GIG is performing in relationship to the operational requirements of the supported missions. Developing and implementing common NetOps metrics will not only significantly improve reporting, especially across organizational boundaries, but will also make information regarding the health of the GIG much more understandable and useful to Commanders and decision-makers at all levels.

4.2   Goal 2: Unify GIG Command and Control

Adopt a unified C2 approach for agile and proactive management of the GIG.

4.2.1 Objective: Provide capabilities to support proactive and adaptive decision making for the operations and defense of the GIG

Today, NetOps personnel and organizations do not have the technical capabilities necessary to see and react to events in real time. For instance, the performance of a network connection or application may be slowly degrading due to a significant increase in the number of users, but this may not be seen until an actual application failure or network isolation occurs. Development and planning of responses is also delayed by existing manual coordination and collaboration techniques used among stove-piped organizations and systems. DoD lacks the dynamic technical and operational capabilities that are needed to enable NetOps personnel to react to rapidly changing and uncertain situations using real-time data.

Moving toward proactive and adaptive GIG management will require improved information sharing and collaboration. It will require automated capabilities that can help operators to quickly identify and assess the potential impact of mission requirements or GIG events, assess alternatives, and present decision makers with viable courses of action for prevention, mitigation or recovery actions. Existing manual NetOps processes and procedures will have to evolve and be supported and, where it makes sense, should be replaced with automated management, control, and decision support and planning capabilities.   In addition it is important for NetOps personnel to engage with operational planners on how modeling and simulation techniques could be used to assess the impact of alternative scenarios and force employment plans on GIG requirements. Using modeling and simulation to anticipate and quickly and accurately explore different responses to a broad range of events will serve to improve GIG effectiveness and responsiveness.

4.2.2 Objective: Implement a GIG management approach that is centrally directed with decentralized policy-based execution for synchronized operations and defense of all GIG domains

Dynamically coordinating management actions across all GIG domains is a major challenge due to the growing complexity of the GIG and the interdependence of assets under the control of different Commanders. Managing this environment requires a decentralized, policy-based approach for executing in a manner that ensures operators at all levels will be empowered to share information, collaborate, and take initiative consistent with the Commander's intent as it is reflected in policy guidance and in automated, policy-based management mechanisms.

Distributed control capabilities will be needed to complement increased situational awareness and enable Commanders and operators to implement needed changes to GIG configurations in a timely manner. Commanders must have the ability to decide: (1) which decisions are to be delegated, and (2) the content of the policy under which delegated decisions will be carried out. In some cases, the policies will be embedded in the systems being controlled.   Some commercial technologies are available to enable distributed, automated, policy-based decision-making, but it will also be necessary to look for and exploit new and emerging technologies.

It is equally important that NetOps have the ability to educate and inform Commanders about the resources that they cannot change. For instance, there are certain aspects of network routing that a Commander could change; however doing so might isolate their network or

unknowingly isolate some other organization's network from critical resources and capabilities. Automated, net-enabled, centralized direction of shared assets and decentralized execution of commands will require major technical, organizational, and cultural changes. However, the result will be more agile, resilient, and responsive GIG support to all missions.

4.2.3   Objective: Develop and adopt consistent and coordinated tactics, techniques, and procedures for NetOps

The GIG is a federation of heterogeneous domains that crosses multiple areas of responsibility and chains of command. Successful command and control of the GIG requires that unity-of-command and unity-of-effort be maintained through improved information sharing, collaboration, and conformance to the Commander's intent. However, ensuring coordination and synchronization of NetOps actions also requires a level of interoperability across different domains. This demands consistent tactics, techniques, and procedures (TTPs) that enable operators to work together. Tabletop and live exercises, modeling and simulation, and operational analyses should be used to rationalize existing TTPs and to develop new ones where necessary to support a unified and Net-Centric approach to NetOps. Rationalization of TTPs is particularly important for the support of Joint operations.

Beyond establishing basic NetOps policy through the development and promulgation of directives, instructions, and manuals, the Department must also develop the doctrine and TTPs necessary to "fight" more effectively by using the GIG as a fully integrated component of Joint warfighting. To meet this end, as the Department implements the National Military Strategy for Cyberspace Operations, synchronization and integration of NetOps becomes even more critical to successful joint operations in the cyberspace domain.

4.3   Goal 3: Institutionalize NetOps

Institutionalize NetOps across DOTMLPF to ensure DoD requirements, acquisition, budgeting, and management processes can be influenced to achieve the NetOps vision.

4.3.1   Objective: Define, develop, and deploy time-phased NetOps capability increments

Achieving the envisioned NetOps target state requires the development of a NetOps transition that is consistent with and supportive of the Defense Information Enterprise Transition Plan (DIETP) and the Capability Delivery Increments (CDI)[7] associated with the Net-Centric portfolio. In the past, NetOps capabilities have many times been added to a system as an afterthought (often as a standalone capability) or left out entirely in favor of added "functionality." This approach has resulted in a basic lack of management and control capabilities, which significantly limits the ability of existing NetOps organizations to fully support the warfighter. Therefore, it is imperative that as Net-Centric capabilities are defined, developed and deployed, their associated NetOps capabilities are concurrently defined, developed, and deployed. Addressing associated NetOps capabilities is, therefore, a mandatory component for each new Net-Centric capability increment.

---

[7] Joint Net-Centric Operations, Capability Delivery Increments; Version 2.0, 19 March 2008

4.3.2 Objective: Develop and implement a standardized GIG Configuration Management process

One of the problems that DoD continues to wrestle with is the lack of a common approach and set of processes for capturing and maintaining configuration management of GIG resources which impacts both GIG security and operational performance. For the Department to realize the full value of the GIG, will require a concerted effort across DoD to develop, implement, and most importantly enforce a comprehensive program of GIG Configuration Management.

4.3.3 Objective: Implement and oversee a NetOps governance structure that supports other Net-Centric strategies.

A governance structure has been introduced in Department of Defense Instruction, *NetOps for the GIG*. It establishes policy and assigns responsibilities for implementing and executing NetOps. A critical aspect of the proposed NetOps governance structure is the creation of implementation plans that respond to this NetOps Strategic Vision by defining the path and steps necessary for NetOps transformation. These plans will ensure that the defined NetOps vision is incorporated into the various stages of NetOps evolution, each of which will be defined, discussed, and agreed upon by the stakeholders, under the oversight of an appropriate governing body.

5 Next Steps

Implementing this Strategic Vision will require that NetOps Implementation Plans be developed and executed at all levels across the Department to address planning, defining, funding, acquiring, and operating NetOps capabilities. These plans will be shaped by the NetOps requirements for each Net-Centric capability increment, and developed and executed to meet the timing of the Net-Centric capability increment's deployment. Approaching the implementation of NetOps incrementally will enable developers and policy makers at all levels to focus their efforts. Policies, architectures, implementation strategies, and deployment schedules can be established to meet specific capabilities that have been identified for each increment. This more focused approach will result in better and timely results.

Future NetOps Implementation Plans must address three key areas: governance through direction and guidance; implementation plans for applying the DoD Net-Centric Data and Services Strategies to NetOps; and NetOps metrics for monitoring, affirmation, and remediation.

6 Conclusion

The Department of Defense must embark upon a coordinated effort to conceive, design, implement, and operate the full range of NetOps capabilities that will be needed to operate and defend the GIG for today and tomorrow. To achieve a GIG that is operated and defended in a way that supports the warfighting, business and intelligence users in any operational environment or mission scenario will require active participation from across a broad cross-section of the DoD. The Department must place increased emphasis on developing and implementing policy and governance to enforce the adoption and implementation of the

capabilities required to achieve the NetOps Strategic Vision. It is intended that this NetOps Strategic Vision will continue to be refined as the GIG continues to evolve toward a seamless, collaborative, and Net-Centric environment.