2006
Department of Defense
Chief Information Officer
Strategic Plan Version 1

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

DoD Chief Information Officer

Preface

The Department of Defense is transforming to become a Net-Centric force. This transformation hinges on the recognition that information is one of our greatest sources of power. Information is a strategic component of situational awareness which enables decision makers at all levels to make better decisions faster and act sooner. Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it is at the heart of Net-Centricity.

As stated in the *DoD National Defense Strategy of the United States of America*, "Transforming to a network centric force requires fundamental changes in processes, policy, and culture. Change in these areas will provide the necessary speed, accuracy, and quality of decision-making critical to future success." From an information perspective, this transformation is embodied in the Net-Centric Global Information Grid (GIG).

The DoD Chief Information Officer (CIO) provides the leadership to meet the Net-Centric vision and ultimately delivers the critical enabling capabilities required by the National Defense Strategy against an evolving threat from both internal and external sources. The 2006 DoD CIO Strategic Plan identifies actions that are critical to transforming DoD operations from platform/organization-centric to Net-Centric. This document is intended to provide a common understanding of the near and mid-term actions required to meet the vision and extend Net-Centricity across the Defense Information Enterprise. The actions described and requested encompass the full breadth of the transformation and include doctrine, organization, training, materiel, leadership/education, personnel and facilities (DOTMLPF) implications.

Achieving the Net-Centric transformation requires an enterprise cultural perspective. Participation and collaboration both within DoD and across non-DoD organizations are critical elements of success. Roles must be clearly defined and responsibilities identified. The actions identified in this document represent near-term steps crucial to our long-term vision – *Deliver the Power of Information: Access - Share - Collaborate.*

Sincerely,

John G. Grimes
DoD CIO

I. INTRODUCTION

Purpose

This *DoD CIO Strategic Plan* identifies key actions and organizational responsibilities that are necessary for the DoD to achieve the transformation from platform/organization-centric to Net-Centric operations.

Transform America's national security institutions to meet the challenges and opportunities of the twenty-first century.

Background

The Department of Defense (DoD) has embarked on a major transformation from its current state of platform/organization-centric operations to Net-Centric operations. The 2006 *Quadrennial Defense Review (QDR) Report* [4] recognizes the importance of achieving Net-Centricity as key to "harnessing the power of information connectivity." Implementation of the Global Information Grid (GIG), in conjunction with evolving technology, operational concepts and culture, is guiding this transformation. The following major goals of Net-Centric operations are driving this transformation:

- Make information available on a network that people depend on and trust.
- Populate the network with new, dynamic sources of information to defeat the enemy.
- Deny the enemy advantages and exploit weaknesses.

We will conduct network-centric operations with compatible information and communications systems, usable data, and flexible operational constructs.

As stated in The *DoD National Defense Strategy of the United States of America*, March 2005 [2], "Transforming to a network centric force requires fundamental changes in processes, policy, and culture. Change in these areas will provide the necessary speed, accuracy, and quality of decision-making critical to future success. Beyond battlefield applications, a network centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes by giving all users access to the latest, most relevant, most accurate information."

The transformation to Net-Centric operations will be achievable only if all aspects of doctrine, organization, training, materiel, leadership/education, personnel and facilities (DOTMLPF) are considered. All too often, the transformation to Net-Centricity focuses only on "materiel" solutions. However, all aspects of DOTMLPF make a vital contribution toward a successful Net-Centric transformation.

The DoD is making progress toward the achievement of its Net-Centric transformation in several areas: determining goals and objectives, articulating policies and guidance, defining operational concepts and initiating programs, establishing organizational responsibilities, and deploying capabilities, including some that are aiding military operations in Iraq and Afghanistan now as well as for future Net-Centric operations and warfare.

Policies and guidance have been provided to develop this required capability, as evidenced by the publication of a series of documents, including the *Global Information Grid Mission Area Initial Capability Description* [5], *Net-Centric Operations and Warfare Reference Model* [6], *DoD Information Technology Standards Registry* [7], *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)* [8], *DoD Net-Centric Data Strategy* [9], and DoD Directive 8320.2, *Data Sharing in a Net-Centric Department of Defense* [10]. Additionally, DoD is developing enterprise and system architectures using the *DoD Architecture Framework*, Version 2.0 [11], and establishing both long-standing and ad hoc Communities of Interest (COIs) for promoting Net-Centric data sharing in support of the above direction, and

beginning to manage the GIG as portfolios of related information technology investments.

Several major programs and initiatives that lay the infrastructure foundation for Net-Centric operations are well underway. These include Global Information Grid Bandwidth Expansion (GIG-BE) (supported by the *High Assurance Internet Protocol Encryptor Interoperability Specification* (HAIPE IS) [12]) , Joint Tactical Radio System (JTRS), Transformational Satellite Communications System (TSAT), Net-Centric Enterprise Services (NCES), and the GIG Information Assurance Portfolio (GIAP) development activities. The Military Services have established major initiatives to advance Net-Centric capabilities, including the Army's LandWarNet, the Air Force's Command and Control (C2) Constellation, and the Navy's FORCEnet. The defense intelligence agencies are taking similar steps within the broader Intelligence Community (IC), both collectively (e.g., the Department of Defense Intelligence Information System (DoDIIS)) and individually (e.g., the National Geospatial-Intelligence Agency GeoScout program and participation in the Distributed Common Ground/Surface System (DCGS)).

Finally, ongoing training and experimentation during the past several years, in addition to events such as the Joint Expeditionary Force Experiment and the Horizontal Fusion Quantum Leap demonstrations, have provided opportunities to explore emerging concepts and the application of new technology such as Service Oriented Architectures (SOA). Active participation in OMB's E-Government initiative is improving DoD's coordination with other government organizations which will allow improved sharing of information across the Federal community.

During the development of this Strategic Plan, the DoD CIO received input from the mission areas (Warfighter, Enterprise Information Environment, Business, and Intelligence). Additionally, the ASD (NII)/ DoD CIO and Joint Staff DJ6 Memorandum, *Broad NII-J6 Network-Centric Concerns* [13], served as a source for identifying and describing the issues addressed herein.

Document Organization

This document identifies and is organized to describe nine areas for focus where the DoD CIO deems actions are necessary to complete the transformation to Net-Centric operations and achieve the value proposition of this transformation.

Each area for focus includes a description of issues or needs that led up to its formulation. Next is a list of actions, grouped as near-term and foundational, that the DoD CIO Strategic Plan calls for specific organizations to perform in moving forward. Near-term actions are those that can be accomplished within a two-year period. Foundational actions are also expected to occur within the near-term timeframe but are ongoing and will require a longer time to accomplish. Finally, the applicable components of DOTMLPF have been identified for each action.

...creation of a collaborative information environment that facilitates information sharing, effective synergistic planning, and execution of simultaneous, overlapping operations... on demand to defense policymakers, warfighters and support personnel.

Summary of Areas for Focus

- **To accelerate the transition to a Net-Centric warfighting culture,** operational concepts and tactics, techniques, and procedures (TTPs) that take advantage of improved information-sharing capabilities must be developed.
- **To make information a force-multiplier,** active Communities of Interest (COIs) must implement the Net-Centric Data Strategy through services that make information discoverable, accessible, understandable and trusted.
- **To provide a secure information environment,** NSA must conceive and establish compelling programs and drive development and implementation of GIAP capabilities that provide the necessary IA functionality.
- **To network the warfighter,** the operating environment must evolve based on the DoD's major networking and C2 programs and coordinated Net-Centric operations procedures.
- **To facilitate warfighter access to intelligence data,** networks and IA technologies and policies need to be developed in collaboration with DNI CIO to permit secure information sharing between the Warfighting and Intelligence Communities.
- **To train the way we'll fight,** training scenarios must capture the benefits of information sharing and risks of Information Warfare.
- **To achieve agility with non-DoD partners,** policies, procedures, and techniques need to be developed that enable the DoD to share information securely outside the ".mil" domain.
- **To capture savings through wise IT investments,** effective portfolio management (PfM) must be implemented in all IT Mission Areas. PfM will serve as a key cross-program, process, and organization integrating and synchronizing activity that will maximize outcomes and minimize costs for DoD missions.
- **To support DoD business process improvement,** DoD must ensure its IT infrastructure is sufficient to support cross-component business process enhancements.

II. AREAS FOR FOCUS

1. ACCELERATE A NET-CENTRIC WARFIGHTING CULTURE: Develop operational concepts that exploit the power of emerging information sharing capabilities and validate these concepts through experiments and warfighting demonstrations.

In the Chairman's assessment of the 2006 QDR, General Pace states "The QDR identifies many areas and technologies that promise to revolutionize the future force. However, transformation is as much a mindset and culture as it is a technology or a platform."

As Net-Centric capabilities and technologies such as Internet Protocol (IP) and Web Services are further developed and deployed, the warfighting culture needs to adopt processes and procedures that exploit these capabilities and take advantage of the new information-sharing paradigms, as called for in the *DoD National Defense Strategy*. To this end, the DoD Net-Centric vision needs to be socialized department-wide through development of Joint and Military Service-specific operational concepts and demonstrations. Increased emphasis must be placed on educating the DoD workforce on the benefits of implementing more efficient processes enabled by the power of Net-Centricity. Joint Force commanders must understand the potential of the network to enhance knowledge sharing, which will improve their ability to act. Benefits need to be understood by staff making funding decisions, preparing policies and directives, and developing strategies for conducting military operations.

One area of specific need is improved understanding of the expected benefits of Net-Centric capabilities within the tactical community. A fundamental objective in the DoD's Net-Centric data strategy is to move "power to the edge." The edge refers to the individual operator or user who might be an intelligence analyst at a Combatant Command, a human resources specialist at a military base, or a warfighter on the streets of Baghdad, Iraq. The deployed warfighter has the greatest need for timely, relevant, and accurate information and, in many cases, is the best provider of information to support accomplishment of the mission. Therefore, TTPs are needed that will enable the warfighter to take advantage of Net-Centric capabilities.

...transformation is as much a mindset and culture as it is a technology or a platform."

Not only does this cultural issue apply to the operational community, but also to the budgeting and acquisition communities. Presently disjointed approaches to identifying, acquiring, engineering, developing, testing, evaluating, integrating and fielding joint and coalition Command, Control, Communications and Computer (C4) capabilities need to be coordinated. DoD is using roadmaps to show the evolutionary path that warfighting capabilities will follow to achieve DoD transformation objectives. These roadmaps must establish milestones for achieving

cultural changes will foster the development of architectures that promote joint interoperability.

Net-Centric capabilities in support of the required operational capabilities. Net-Centric concepts need to be institutionalized throughout the Joint Capabilities Integration and Development System (JCIDS), Defense Acquisition System (DAS), and Planning, Programming, Budgeting and Execution (PPBE) processes, as well as during operational planning and execution. These cultural changes will foster the development of architectures that promote joint interoperability. New governance approaches and effective systems engineering of both the overall GIG and individual programs are essential.

A suggested method for promulgating the benefits of Net-Centric operations is to conduct experiments, pilot programs, demonstrations, and exercises. Additionally, the research and development capabilities of the industrial and educational communities will contribute through development of innovative and advanced Net-Centric capabilities. Allowing the warfighter to have hands-on experience with new capabilities will help demonstrate the value of improved information-sharing techniques and provide crucial feedback to the acquisition community based on the warfighter's perspective. During operational experiments and exercises, the use of innovative Net-Centric concepts and technologies by the warfighter should be encouraged. As these concepts and technologies mature, more rapid ways to insert them into the operational environment will be needed. Pilot implementations of new capabilities can provide the opportunity to assess their feasibility within a limited operational environment. Demonstrations normally serve as tools that convey progress and garner necessary support to move complex systems forward.

The DoD CIO calls for the following actions:

Near-Term Actions

a. Joint Forces Command: Establish a joint forum for developing operational concepts and TTPs that take advantage of improved information-sharing capabilities. (Doctrine)

b. USD (AT&L) and the Joint Staff: Continue to lead the development of capability area roadmaps to support enterprise-level synchronization across programs and support early deployable Net-Centric capabilities. (Materiel, Leadership)

c. Combatant Commanders and Office of Force Transformation: Share lessons learned regarding operational use of Net-Centric capabilities to include those from Iraq and Afghanistan. (Training, Leadership)

d. DoD CIO together with National Defense University: Provide widely accessible education and training for the DoD workforce that promotes the benefits of Net-Centricity. (Training, Leadership)

e. DoD CIO and Joint Staff J-6: Establish a DoD policy that provides incentives for the identification of Net-Centric opportunities (for immediate to 6-month implementation) which rapidly improve warfighting, support, and business processes. (Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities)

Foundational Actions

f. Military Services and Combatant Commands: Conduct joint experiments, pilot programs, demonstrations, and exercises that show the value added by using Net-Centric capabilities. (Doctrine, Training)

g. DoD CIO and DDR&E: Guide and Monitor research and development capabilities of the industrial and educational communities to promote development of innovative and advanced Net-Centric capabilities. (Leadership)

h. Military Services and Agencies: Investigate technological solutions, process changes, and organizational alignment and training adjustments to address shortfalls that could impede the Net-Centric transformation of military operations. (Organization, Training, Leadership)

2. MAKE INFORMATION A FORCE MULTIPLIER: Ensure that data is visible, accessible, understandable, and trusted, when and where needed to accelerate decision- making during military operations.

The 2006 QDR recognizes the need for DoD to "...strengthen its data strategy... to improve its information sharing ... across a multitude of domains.

The 2006 QDR recognizes the need for DoD to "...strengthen its data strategy...to improve its information sharing ... across a multitude of domains." The DoD Directive 8320.2, *Data Sharing in a Net-Centric Department of Defense* [10], and the *DoD Net-Centric Data Strategy* [9] goals include making data visible, accessible, understandable, trusted, and interoperable. These goals require methods of providing data discovery, data asset interoperability, data security marking, context metadata, pedigree metadata, and data quality. They especially require an improved understanding of the meaning of data, so that users and programmers will correctly interpret data as it crosses system and organizational boundaries. The DoD CIO's Net-Centric Operations and Warfare Reference Model (NCOW-RM) provides definition of the tasks required to implement these goals.

The DoD must realize the efficiencies to be gained by understanding the meaning of data and using it in a way that maximizes the effectiveness of military operations. However, increasing the amount of information available during military operations always poses the risk of information overload. The DoD must implement edge user tools or capabilities that act as directed information retrieval tools and information filters for the warfighter. These agents would discover, interpret, and sort the data according to designated parameters to eliminate unwanted data and present high-priority data first.

A need exists for further development of the COI concept and coordination of metadata registries that provide common structure and meaning of data to facilitate information sharing among DoD, Intelligence, and Department of Homeland Security (DHS) organizations, coalition partners, and non-governmental organizations. COIs are "data planning cells," either long-standing or ad hoc, within and across mission areas and programs. Each COI is expected to develop a common data model for information exchange and to place the data strategy into action through the COI members and mission area owners. Additionally, the DoD must identify the governance process for COIs and determine the degree of information integration needed. To help facilitate COI development, a capability must be established which enables COIs to discover the lessons learned by COI pilots.

The DoD CIO calls for the following actions:

Near-Term Actions

a. DoD CIO: Develop a detailed plan to implement the DoD Net-Centric data strategy across warfighter, business, intelligence, and enterprise information environment mission areas. (Leadership (Policy))

1. DoD CIO. Continue to define COI roles, governance, missions, products, and relationships to other entities. (Organization, Leadership (Policy))
2. DoD CIO: Continue to promote establishment of long-standing and ad hoc COIs. (Organization)
3. DoD CIO: Continue to promote the implementation and reuse of metadata registries supporting data discovery. (Materiel)
4. COI leads: Develop a common data model for information exchange to be used by their COI members and processes. (Organization, Training, Materiel, Leadership (Policy))
5. DoD CIO: Establish a capability that enables COIs to discover the lessons learned by COI pilots. (Leadership)

b. Military Services and Agencies: Develop and implement edge user tools or capabilities that address information discovery and filtering for the warfighter. (Materiel)

c. Military Service and Agency program managers: Identify data dependencies and develop mitigation plans to address gaps. (Materiel, Leadership (Policy))

Foundational Actions

d. Military Services and Agencies: Implement discovery and data content tagging to facilitate information sharing and understanding of the data. (Materiel)

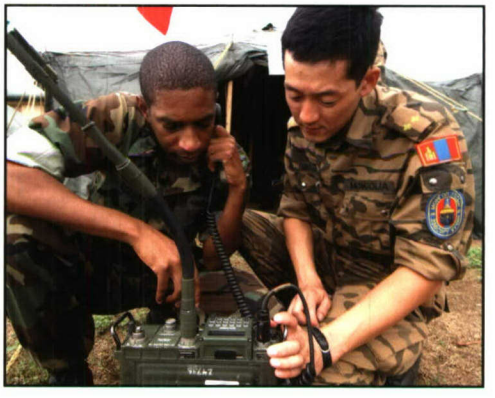
e. Military Services and Agencies: Account for processing and bandwidth implications of data tagging in designs. (Materiel)

f. COI leads: Develop a set of measurable IT system performance metrics to evaluate accomplishment of the processes involved in executing the Joint Capability Areas. [14]. (Leadership (Policy))

3. SECURE THE NET: Enable the National Security Agency (NSA) to implement the GIAP.

IA initiatives must be incorporated into new capabilities from their inception to ensure mission success.

The goal of securing the net is mission assurance. The 2006 QDR identifies that DoD will "...defend and protect information and networks and focus research and development on its protection." Critical DoD and Intelligence Community systems, networks, platforms, and sensors should not be developed and deployed without the necessary security and interoperability capabilities. The essential tenets of mission assurance include protecting information, defending and keeping networks operational, acquiring trusted software, providing integrated situational awareness, transitioning and enabling IA capabilities, and creating an IA-empowered workforce. Because of the importance of protecting intelligence information to national security, DoD CIO and Director for National Intelligence (DNI) CIO must partner closely to develop compatible strategies for assured information sharing. To this end, the DoD CIO, in collaboration with the DNI CIO, is spearheading several initiatives to strengthen IA across the entire DOTMLPF range. These IA initiatives must be incorporated into new capabilities from their inception to ensure mission success.



To this end, mechanisms are being put in place to enable NSA to implement an IA capabilities portfolio known as the GIAP that provides the necessary IA functionality to support a Net-Centric environment. NSA must develop near-term IA policies, plans and programs for enterprise security services.

Since DoD depends on commercial software, an important aspect of the GIAP is to ensure that the software is trustworthy and free from bugs and vulnerabilities. DoD is developing and implementing a software assurance strategy that leverages and collaborates with industry to promote methods for providing highly assured software and software-enabled technologies. Repeatable systems engineering processes are needed to assess, isolate, and mitigate software assurance vulnerabilities. DoD will continue to work with commercial vendors to acquire services and technologies quickly. An efficient governance structure will be implemented that ensures consistent implementation of GIAP standards and mediates exceptions that change the mission risk posture of the community.

The DoD CIO calls for the following actions:

Near-Term Actions

a. NSA: Develop new methods to streamline certification and accreditation to expedite delivery of capabilities and expedite insertion of new technologies without compromising the integrity of the GIG. (Organization, Materiel, Leadership (Policy))

b. DoD CIO: Establish policy that defines criteria for accepting network access credentials of non-DoD organizations. (Leadership (Policy))

c. NSA: Develop near-term GIAP policies for enterprise services. (Leadership (Policy))

d. Implement a DoD software assurance strategy, to include the following actions:

1. DoD CIO: Lead the effort to leverage and collaborate with industry to promote a national industrial base that provides highly assured software and software-enabled technologies. (Materiel)
2. NSA: Identify the most important capabilities and selected critical components for attention. (Materiel)
3. NSA: Evaluate the threat and assess security-related practices of suppliers of critical components. (Materiel)
4. NSA: Employ repeatable systems engineering processes to assess, isolate, and mitigate software assurance vulnerabilities. (Materiel)

e. DoD CIO: Appoint NSA, working with the Director, Defense Research and Engineering (DDR&E), as DoD executive agent for software vulnerability mitigation and discovery to focus science and technology on research and development of technologies that will identify vulnerabilities and improve assured software development practices. (Materiel)

f. NSA: Complete and use the GIAP to manage delivery of IA functionality in support of Net-Centric Operations.

1. DoD CIO: Establish mechanisms that enable NSA to implement the GIAP. (Leadership (Policy))
2. NSA: Develop an Identity Management approach that meets the needs of DoD users, especially those working at the tactical edge, and non-DoD users (e.g., DHS). (Materiel, Leadership (Policy))
3. NSA: Lead the IA community with support from DDR&E to establish a comprehensive research and technology strategy and roadmap to address challenging GIAP problems. (Leadership (Policy))

g. Military Services and Agencies: Create an IA-empowered workforce by implementing DoD Directive 8570-1M, *IA Training, Certification and Workforce Management Policy* [15]. (Training)

Foundational Actions

h. DoD CIO: Partner closely with DNI CIO to develop compatible strategies for assured information sharing. (Leadership)

i. NSA: Establish an all-source threat assessment capability to analyze threats posed by software suppliers. (Materiel)

j. NSA, in cooperation with DHS: Establish a National Technology and Evaluation Center. (Organization, Facilities)

k. DIA: Strengthen analysis capability of emerging threats to DoD IT and improve dissemination of this information to the operating, training and acquisition communities. (Training, Materiel, Personnel)

l. NSA: Develop common "Protection Profiles" so that IA certifications are consistent across the third party labs. (Leadership (Policy))

4. NETWORK THE WARFIGHTER: Provide an operating environment based on the DoD's major networking and C2 programs and coordinated Net-Centric operations procedures.

Building capabilities that support joint Net-Centric operations has been underway for several years. DoD Military Services and Agencies have identified key programs in communications/transport, information assurance, computing, applications, storage, and service-oriented architectures that are required to realize the full potential of information sharing. The DoD must continue to support these development activities through use of Enterprise-Wide System Engineering (EWSE) processes, understanding the interrelationships among the various components that will eventually provide end-to-end capabilities during military operations.

The major programs and initiatives that need continued support include the Defense Information Systems Network (DISN) and its GIG BE expansion, JTRS, TSAT and NCES. The Military Services will need to continue development and modernization of connections to the GIG backbone as well as the development of their major initiatives in Net-Centric operations including the Army's LandWarNet, the Air Force's C2 Constellation, and the Navy's FORCEnet. As a guiding principle, acquisition programs should be evaluated based on their consistency with the Net-Centric tenets and the evolving GIG spirals and architectures, such as Service Oriented Architecture (SOA). A major tenet of SOA is the transparency across component boundaries of not only enterprise services but also COI-specific services.

In implementing its SOA, DoD must give special attention to the development of information systems, enterprise and COI-specific services and communications capabilities that are built on Net-Centric principles and address the unique needs of the joint tactical community. Whether in a vehicle or on foot, the warfighter at the tactical edge is highly constrained by spectrum, bandwidth, processing, and user interface considerations.

The Joint Staff (J-6), ASD(NII), USD (AT&L), USSTRATCOM, USJFCOM and DISA have embarked on several efforts to define capability needs and to synchronize and manage development and fielding of programs which comprise the GIG operating environment. The Enterprise Information Environment Mission Area (EIEMA) defines a portfolio of programs that address information transport, core enterprise services (to include directory services), information assurance, and computing. The recently defined Joint Capability Area (JCA) called Joint Net-Centric Operations (JNO) will provide a timely, synchronized, integrated and cost-effective end-to-end

enabling capability driven by the needs of warfighters and their associated user applications. JNO is mainly comprised of programs that make up the EIEMA portfolio. By managing the programs of the EIEMA portfolio on a capability basis as framed by the JNO JCA, DoD will be able to deliver the necessary cross-domain Net-Centric capabilities in a synchronized and cost effective manner. To this end, DoD must establish a JNO Capability Portfolio Manager to identify and balance validated warfighter capability needs and lead the development of solutions to meet those needs across the range of DOTMLPF.

Dependent upon the capabilities provided by the JNO portfolio are warfighter/user applications to support C2, logistics and battlespace awareness. A recently defined JC2 portfolio, comprised of programs such as Net-Enabled Command Capability (NECC), Global Command and Control System (GCCS) family of programs, Combatant Commanders Integrated Command and Control System (CCI2S) and others, will deliver necessary C2 capability to the warfighter. To ensure delivery of an effective end-to-end capability, the JNO and JC2 portfolios will be synchronized and coordinated.

JNO includes the framework employed to operate and defend the GIG to ensure information superiority, commonly referred to as NetOps. A NetOps strategy needs to be developed that describes a set of NetOps goals and actions that must be met to achieve the vision of a GIG capable of supporting the DoD's Warfighting, Defense Intelligence and Business Mission Areas. NetOps' essential tasks for the GIG are enterprise management, network defense, and content management which provide assured system and network availability, information protection, and assured information delivery. As different components of the JNO JCA are developed, NetOps needs to be coordinated and resourced across DoD, with particular emphasis on tactical environments. This activity includes development of capabilities to establish and sustain joint configuration management and situational awareness of the GIG. The associated planning, research and development should also be conducted with greater focus on efficient use of the electromagnetic spectrum.

...a mechanism must be created to prevent architectural differences among LandWarNet, C2 Constellation and FORCEnet from creating performance and interoperability problems...

In support of military operations, a mechanism must be created to prevent architectural differences among LandWarNet, C2 Constellation and FORCEnet from creating performance and interoperability problems within the GIG. In addition, a common architecture and set of Service Level Agreements (SLAs) must be developed to enable providers and consumers to measure the quality of service (QoS) as part of NetOps. Specifically, prioritization schemes that are capable of handling disparate data streams (e.g., data, voice, and video) must be developed and implemented, consistent with the findings of the Enterprise-Wide System Engineer (EWSE). A NetOps data strategy is needed that allows for definition of both tight and loose information dependencies among systems.

The DoD CIO calls for the following actions:

[1] JNO is expected to supersede the term NCOE in future versions of the Joint Functional Concept and JIC documents and elsewhere. JNO is already in use along with other JCAs by PA&E in annotating the FYDP for analysis and other purposes.

Near-Term Actions

a. Military Services and Agencies: Budget for the development of key Net-Centric programs and initiatives. (Materiel)

b. ASD (NII) in coordination with the Joint Staff J-6: Maintain and evolve the NCOE roadmap into a broader JNO roadmap. (Materiel, Leadership (Policy))

c. ASD (NII), USSTRATCOM, and USJFCOM: Advocate establishment of a JNO capability portfolio manager. (Organization, Materiel, Leadership(Policy))

d. Command and Control Capabilities Integration Board (C2CIB), ASD(NII), USSTRATCOM, and USJFCOM: Synchronize and coordinate JNO and JC2 portfolios (Materiel, Leadership(Policy))

e. DoD CIO, USSTRATCOM and Defense Information Systems Agency (DISA): Develop the DoD NetOps strategy, as part of JNO, that describes a set of NetOps goals and actions that support the DoD's Warfighting, Intelligence and Business Mission Areas. (Doctrine, Leadership (Policy))

f. ASD (NII), USSTRATCOM and DISA: As part of JNO, coordinate and resource NetOps across DoD, with particular emphasis on tactical environments. (Organization, Materiel, Leadership (Policy))

1. Establish and sustain joint configuration management.
2. Establish and sustain situational awareness capabilities for the GIG.
3. Use and perform R&D to make better use of DoD portion of electromagnetic spectrum.

Foundational Actions

g. DoD CIO: Lead alignment of the GIG architectural implementations of the components (e.g., LandWarNet, C2 Constellation, and FORCEnet). (Materiel, Leadership)

h. USSTRATCOM and DISA: Develop prioritization schemes to ensure that communication assets are allocated to information requirements on the basis of their criticality to mission success and develop SLAs that enable providers and consumers to measure QoS as part of NetOps. (Doctrine, Leadership (Policy), Materiel)

i. DoD CIO: As a guiding principle, continue to evaluate acquisition programs based on the Net-Centric tenets and the evolving GIG spirals and architectures. (Materiel, Leadership (Policy))

5. FACILITATE WARFIGHTER ACCESS TO INTELLIGENCE DATA: Implement networks and develop IA technologies and policies in collaboration with the DNI CIO that facilitate secure information sharing between the Warfighting and Intelligence communities.

The DoD National Defense Strategy emphasizes the importance of sharing intelligence information. Consequently, DoD in cooperation with DNI is adjusting policies, modifying practices, and implementing tools such as DCGS to make quality intelligence data, both raw and processed, more widely and rapidly available to the warfighter.

An essential tenet of Net-Centric operations is the ability to provide rapid access to the right information at the right time in a form that is immediately useful, thus giving U.S. forces information and decision superiority. Information sharing involves significant challenges relating to information security; these challenges have been highlighted as DoD moves from a culture of "need to know" to one of "role-based access," especially when applied to joint, multinational, and multi-agency environments. Building a secure, seamless network that responds to the vision of Net-Centric operations calls for a new and innovative approach to security risk management and a coordinated NetOps capability. This approach is especially important for effective intelligence information sharing.

Development of requirements, guidelines, and new programs and technologies is an immediate and critical need. An important step in these development activities is the agreement on a cooperative governance structure. The coordinated implementation of information-sharing techniques among the DoD warfighting, DoD Intelligence and DNI communities is tightly coupled with long-term GIAP objectives, including multi-level domain architectures and dynamic policy management. Many of the required techniques are well beyond current IA technology capabilities, and research is needed in these areas. These efforts must allow for the DoD and IC information environments to survive professional-grade cyber attacks while maximizing the ability to share multi-level information across joint and multinational forces and multiple agencies.

The DoD CIO calls for the following actions:

An essential tenet of Net-Centric operations is the ability to provide rapid access to the right information at the right time in a form that is immediately useful...

Near-Term Actions

a. USD (I) and DoD CIO: Lead the development of a common DoD IC vision for two-way information sharing. (Leadership (Policy))

b. USD (I) and DoD CIO: Lead the development of a coordinated DoD warfighting, DoD Intelligence and DNI data sharing governance structure. (Doctrine, Leadership(Policy))

c. DoD CIO: In cooperation with DNI and DoD IC, continue to coordinate enterprise service development to facilitate collaboration, discovery, messaging, mediation, and user assistance. (Doctrine, Materiel, Leadership(Policy))

d. USD (I), DoD CIO and USSTRATCOM: Lead the development of coordinated NetOps capabilities, including the operational aspect of the GIAP to facilitate information sharing and to protect assets from sophisticated cyber attacks. (Organization, Materiel, Leadership (Policy))

e. USD (I) and DoD CIO: Develop an intelligence data COI and coordinate metadata registries. (Organization, Leadership (Policy))

Foundational Actions

f. USD (I) and DoD CIO: Continue to synchronize information sharing techniques. (Materiel, Leadership (Policy)

6. TRAIN THE WAY WE'LL FIGHT: At all levels, routinely conduct exercises and training using scenarios that capture the benefits of information sharing and also include an adversary that is aggressively trying to exploit DoD's use of information technology.

Effective use and sharing of information will place an ever greater reliance on networks and network-enabled services during military operations. This reliance has raised concerns about the interoperability and security of systems regarding information attack and exploitation. Even in open literature, our potential adversaries are discussing their plans to exploit Information Warfare (IW). In 2002, Congress directed that "each Combatant Command and Military Service ensure that robust C4ISR functionality is included annually within at least one of its major exercises… (and) that an operational evaluation of interoperability and information assurance be conducted during these exercises." [17]

Therefore, DoD must dedicate resources to promote a realistic perspective on how to train and exercise forces and organizations. To win militarily in the new global environment, DoD users must be trained effectively to overcome decisively asymmetric adversaries and to address surprises. The training system in place today, a product of the 1990s, was designed assuming a well-defined and stable opponent. However, the challenges of today demand replacement of this requirements-driven training system with one that is dynamic, collaborative, and capabilities based.

To capture the full benefit of information sharing, education, training, and exercises need to be refocused toward IT areas. Improved evaluation, certification, and review processes must also be established. The warfighter needs to be trained to use the network to access new information, assist in information fusion, and employ enterprise services (such as discovery and smart agents). The warfighter must learn to fight the network like a weapons system and use support systems more effectively. The warfighter needs to understand and, in training events and exercises, experience adversarial application of information warfare (e.g., attacks and exploitation). Free-play exercises should be conducted regularly to test warfighter flexibility and to identify new, non-traditional ways of using information. DoD must also provide joint training that fosters synergies between the IC and the warfighter. These operational exercises and training will provide the foundation for executing the DoD Net-Centric Data Strategy.

The DoD CIO calls for the following actions:

To win militarily in the new global environment, DoD users must be trained effectively to overcome decisively asymmetric adversaries and address surprises.

Near-Term Actions

a. Military Services and Combatant Commands: Ensure that robust Net-Centric information sharing is included annually in at least one of their major exercises and that operational evaluation of Net-Centric operations, including IA capabilities, is conducted in these exercises. (Training, Leadership)

b. Military Services and Combatant Commands: Use experimentation and concept development, based upon lessons learned during operational missions and training venues, to develop new tactics, techniques, and procedures that exploit the power of Net-Centricity. (Doctrine, Training)

c. STRATCOM, Joint Staff, and USD (P&R): Assess status of IW capabilities within the DoD training community and determine necessary improvements. (Organization, Training, Leadership, Personnel)

d. DoD Training Centers: Include IW threat detection, prevention and response in System Administrator Training. (Training)

Foundational Actions

e. Military Services and Combatant Commands: Use the *Joint National Training Capability* [18] to train forces in the employment of cross-Service information sharing to improve combat effectiveness. (Training)

f. Combatant Commands, Military Service Training Centers, and Information Warfare Centers: Develop new capabilities to allow IW to occur during training events to improve the understanding of the benefits and vulnerabilities of Net-Centric warfare to military operations. (Doctrine, Training)

7. ACHIEVE AGILITY WITH NON-DoD PARTNERS:
Develop policies, procedures, and technologies to share information securely with coalition partners, other federal agencies, and business partners.

As described in the 2006 QDR and called for in the DoD Directive 3000.05 *Security, Stabilization, Transition and Reconstruction*[19], the U.S. warfighter often must work in cooperation with many different non-DoD partners, such as NATO allies, coalition partners established for a specific conflict, federal agencies, non-governmental organizations and the commercial sector. In coordination with USD (P) and USD (AT&L), the DoD CIO is developing policies, procedures and techniques that enable communication, collaboration, translation, and sustainment of engagements outside the ".mil" domain in both trusted and open environments. Also, rapidly deployable capabilities need to be developed for these types of cooperative operations, social networks must be grown, and the concepts need to be incorporated into doctrine.

Challenges of the Net-Centric approach include how to post information to be made available to non-DoD partners and how to develop enterprise services (especially discovery services) that can help DoD's partners find the information they need. For partners with which DoD has continuing relations, the interconnection of DoD and non-DoD assets must be established and tested. For coalitions that are formed quickly, techniques for ad hoc information sharing need to be developed. Additionally, sharing information with these partners is often complicated by use of different IT standards and data formats, different rules for releasing information and protecting network assets, and even use of different languages to communicate among foreign partners.

DoD needs to implement methods to manage the transition from today's information-sharing paradigm, which is focused on interconnecting physical networks separated by classification, to a more Net-Centric paradigm, which allows information sharing on the basis of classification and role-based access. Special attention is being given to the GIAP to promote the development of cross-domain solutions (CDS) which will permit collaboration with first responders, non-governmental organizations (NGOs), state and local governments, as well as coalition information sharing.

The DoD needs to continue active participation in combined experiments, exercises, and demonstrations to help develop the procedures and techniques for information sharing. Examples include the Coalition Warrior Interoperability Demonstrations (CWIDs) with NATO allies and the TOPOFF exercises and its linkages with non-DoD Federal agencies.

The DoD CIO calls for the following actions:

As described in the 2006 QDR and called for in the DoD Directive 3000.05 Security, Stabilization, Transition and Reconstruction[19], the U.S. warfighter often must work in cooperation with many different non-DoD partners...

Near-Term Actions

a. DoD CIO: Identify key non-DoD partners and cooperatively develop secure information-sharing policies. (Leadership(Policy))

b. USSTRATCOM and DISA: Establish gateways to interface non-DoD and coalition networks into the GIG and test these interfaces. (Materiel)

c. Combatant Commands: Coordinate DoD participation in combined experiments, exercises, and demonstrations. (Training, Leadership)

d. ASD (NII), Military Services and Agencies: Coordinate with non-traditional DoD partners to develop rapidly deployable capabilities that enable communication, collaboration, translation, and sustainment of operations. (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities)

Foundational Actions

e. USJFCOM and DISA: Develop techniques for ad hoc information sharing and establish methods for information posting to non-DoD partners. (Doctrine, Materiel)

f. NSA: As part of the GIAP, develop cross-domain solutions (CDS) which will permit collaboration with first responders, non-governmental organizations (NGOs), state and local governments, as well as coalition information sharing. (Material)

8. CAPTURE SAVINGS THROUGH WISE IT INVESTMENTS: Align DoD IT investments with its warfighting and business strategies.

Making wise IT investments is one of the main tenets of the *Clinger-Cohen Act of 1996* [20] and has been a key foundation within DoD for IT systems acquisition for several years. The 2006 QDR states, "As an enterprise asset, the collection and dissemination of information should be managed by portfolios of capabilities that cut across legacy stove-piped systems."

On October 10, 2005 , the Deputy Secretary of Defense signed the *Information Technology Portfolio Management Directive* [21] that established roles and responsibilities in DoD for managing IT as portfolios of investments. These portfolios represent related systems that cross Military Service and Agency boundaries to deliver capabilities to warfighters and others. The concept of portfolio management is to maximize outcomes and minimize costs for DoD investments. Duplicate and legacy systems can be eliminated, saving hundreds of millions of dollars that can be recapitalized to better support military operations. Tradeoffs that maximize the return on IT investment can be more easily made within this framework. Critical to the success of IT Portfolio Management is clearly articulating responsibilities for the development and implementation of IT services and capabilities among the IT portfolios.

The DoD must integrate portfolio management into the major decision systems of the Department, organize effectively to perform portfolio management, and continue to implement techniques to analyze, select, control, and evaluate IT investments. Decisions on which IT investments to make, modify, or terminate must be based on the GIG Architecture [22], mission area goals, risk tolerance levels, potential returns, outcome goals, and performance. All three decision support systems (JCIDS, DAS, and PPBE) must consider and employ portfolio managers' recommendations. For example, the concept of Capability Area Reviews should be extended to include IT portfolios.

The DoD must integrate portfolio management into the major decision systems... to analyze, select, control, and evaluate IT investments.

Integrated architectures and capability delivery plans employing enterprise, mission area, domain, and component-level perspectives must be developed, maintained, and applied to gain a better understanding of the organizational need and the capability gaps between current and future IT portfolios. These architectures and capability delivery plans will be used to assess process improvement opportunities within and across the levels, identify potential duplication, determine interoperability and capability requirements, promote standards, formulate and target investments to improve data and information management, and identify the required capabilities of

the technical infrastructure. DoD will continue to actively participate in OMB's E-Government initiative to identify opportunities to share information with other Federal departments and agencies and to achieve cost savings.

Frequently, use of COTS permits rapid and less costly development of IT solutions. As the GIG moves toward an SOA approach, use of commercial standards that permit discovery and use of web-services will facilitate the department's ability to leverage the advantages of COTS SOA solutions.

DoD needs to develop a means to identify and cross-reference all DoD systems uniquely against their Program Element (PE) codes to enforce policy compliance and provide needed information to assist senior investment decisions properly. This effort must include the ability to trace policy requirements for each program across all functional areas (i.e., budgeting/ Program Objectives Memorandum (POM) development, JCIDS, interoperability, IA/ Federal Information Security Management Act (FISMA) [23] reporting, etc.) back to the appropriate funding source. In support, DoD needs to establish a COI to develop and provide Net-Centric access to data necessary to manage IT investments.

The investment management processes should leverage the DoD's principal decision support systems (i.e., JCIDS, DAS, and PPBE process). The roles and responsibilities of DoD IT stakeholders: Office of the Secretary of Defense (OSD), Joint Staff, Military Services, Combatant Commands, DISA, IC, and Defense Threat Reduction Agency (DTRA) need to be clarified to help reduce duplication of effort and close seams and gaps.

Near-Term Actions

a. Military Services and Agencies: Identify and cross-reference all programs against their PE codes to support policy enforcement and facilitate informed investment decision-making. (Doctrine)

b. DoD CIO: Lead the effort to clarify roles and responsibilities of IT stakeholders to reduce duplication of effort and close gaps. (Organization, Leadership (Policy))

c. DoD CIO: Issue an instruction to follow the approved DoD IT Portfolio Management Directive and extend Capability Area Reviews to include IT portfolios. (Organization, Leadership (Policy))

d. DoD CIO and BTA Leadership: Sustain an IT Management Data Community of Interest to provide Net-Centric access to data necessary for management of IT investments. (Organization, Leadership (Policy))

e. DoD CIO: Organize, resource and articulate services and capabilities of the EIEMA portfolio and associated domain portfolios. (Organization, Materiel, Leadership)

f. DoD CIO: Continue to look for opportunities to align the DoD Architecture to the Federal Enterprise Architecture. (Leadership (Policy))

g. DoD CIO: Develop improved ways to advance best architecture practices within DoD and to share DoD best practices with other government partners. (Training, Leadership (Policy))

Foundational Actions

h. DoD CIO: Continue to organize to execute portfolio management and implement techniques to analyze, select, control, and evaluate IT investments. (Organization, Materiel, Leadership (Policy))

i. Military Services and Agencies: Develop and maintain integrated architectures and capability delivery plans that identify capability gaps and overlaps in current and future IT portfolios. (Doctrine, Organization, Materiel, Leadership (Policy))

9. SUPPORT DOD BUSINESS PROCESS IMPROVEMENT:
Ensure DoD IT infrastructure is sufficient to support cross-component business process enhancements.

...DoD is committed to the deployment of DoD Business Enterprise Capabilities through disciplined program management.

As stated in the DoD BTA's 2006 Annual Report to Congressional Defense Committees: [24] "Today, a seamless defense business infrastructure is critical to support responsive, agile military operations. The goal for Defense Business Transformation is to provide our U.S. Armed Forces, what they need—when they need it—where they need it."

The report further states that the four key objectives of the Department's business transformation efforts are to:

- Provide support for the joint warfighting capability
- Enable rapid access to information for strategic decisions
- Reduce the cost of Defense business operations
- Improve financial stewardship to the American people

In support of the BTA, the DoD CIO will support development of the GIG infrastructure necessary to operate the SOA envisioned by the draft Enterprise Transformation Plan [25], August 4 2006. This infrastructure will enable interoperation and interconnection of business systems and applications when they need to exchange information, expose functionality, or consume information across federation boundaries. Identification and monitoring of Business Enterprise Architecture (BEA) compliance with standards and policies are needed to support Business Mission Area federation with the other DoD Mission Areas.

The DoD CIO calls for the following actions:

Near-Term Actions

None identified

Foundation Actions

a. BTA and DoD CIO: Identify and monitor policies needed to support Business Mission Area federation with the other DoD Mission Areas. (Leadership (Policy))

b. DoD CIO: Support development of the GIG infrastructure necessary to operate the SOA. (Training, Materiel, Leadership)

III. SUMMARY

Effective information sharing is the key to a successful transformation. Information sharing depends on the development of data management and information assurance techniques that are implemented across the DoD, Intelligence Community and our non-DoD partners.

The transformation from platform/organization-centric to Net-Centric operations, as called for in the DoD National Military Strategy, will require the entire spectrum of DOTMLPF to co-evolve as Net-Centric capabilities are implemented. This Strategic Plan has identified nine areas for focus where the DoD CIO deems actions are necessary to achieve Net-Centric operations.

Although materiel solutions that enable information sharing are key, information policy issues must now be addressed to make the most effective use of new capabilities.

Approximately 60% of the actions identified in this document are related to development or adjustment of "Policy." However, this is not to say that policy improvements should be pursued at the expense of IT materiel developments. Only through coordinated improvements to both policy and materiel can the full potential of Net-Centricity be realized in a timely manner.

Finally, to ensure success, the DoD CIO must engage Military Services, Defense Agencies, and COCOM leadership and get their buy-in. This transformation will not happen overnight. But through wise investment decisions, realistic training and strong leadership, the warfighter will have an ever-growing set of Net-Centric capabilities to *Deliver the Power of Information: Access – Share - Collaborate.*

REFERENCES

1. United States Executive Office of the President, *The National Security Strategy of the United States of America*. Washington, D.C., March 2006.
2. United States Department of Defense, *The National Defense Strategy of the United States of America*, Washington, D.C., March 2005.
3. Joint Chiefs of Staff, *The National Military Strategy of the United States of America: A Strategy for Today, a Vision for Tomorrow*, Washington, D.C., 2004.
4. Office of the Secretary of Defense, *Quadrennial Defense Review Report, Washington*, D.C., February 2006.
5. Joint Requirements Oversight Council, *Global Information Grid (GIG) Mission Area Initial Capabilities Document (MA ICD)*, JROCM 202-02, 14 Aug 2004.
6. Office of the Assistant Secretary of Defense for Networks and Information Integration (NII), *Net-Centric Operations and Warfare Reference Model (NCOW-RM) V1.0*, 9, Washington, D.C., Dec 2003.
7. Defense Information Systems Agency, *DISRonline: DoD Information Technology Standards Registry, Baseline Release 06-1-1* [Unclassified]. <https://disronline.disa.mil/a/DISR/index.jsp>.
8. United States Department of Defense, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, DoD Instruction No. 4630.8, June 30, 2004, and *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, DoD Directive 4630.5, May 5, 2004.
9. United States Department of Defense, Chief Information Officer, *DoD Net-Centric Data Strategy*, Memorandum for Secretaries of the Military Departments, Washington, D.C., May 9, 2003.
10. United States Department of Defense, *Data Sharing in a Net-Centric Department of Defense*, DoD Directive No. 8320.2, December 2, 2004.
11. Office of the Assistant Secretary of Defense for Networks and Information Integration (NII), *DoD Architecture Framework*, Version 1.0, February 9, 2004.
12. National Security Agency, *High Assurance Internet Protocol Encryptor Interoperability Specification*, March 31, 2005.
13. LtGen Robert M. Shea, USMC, Director for Command, Control, Communications and Computer Systems, Joint Staff and Linton Wells II, Assistant Secretary of Defense (Networks and Information Integration)/Department of Defense Chief Information Officer (Acting), *Broad NII-J6 Network-Centric Concerns*, Memorandum, Washington DC, May 20, 2005.
14. Secretary of Defense, Memorandum, *Operational Availability (OA) – 05 /Joint Capability Areas*, Washington, D.C., May 6, 2005.
15. United States Department of Defense, *Information Assurance Training, Certification and Workforce Improvement Program*, DoD Directive 8570.01-M, December 19, 2005.
16. Joint Chiefs of Staff, *Net-Centric Operational Environment Joint Integrating Concept, Version 1.0*, Washington, D.C., October 31, 2005.

17. U.S. Congress, House, Committee on Appropriations, *Department of Defense Appropriations Bill, 2003*, 107th Congress, H. Rpt. 107-532, June 25, 2002.

18. Office of Under Secretary of Defense (Personnel and Readiness), *Department of Defense Training Transformation Implementation Plan*, June 10, 2003

19. United States Department of Defense, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations*, DoD Directive 3000.05, November 28, 2005.

20. *Information Technology Management Reform Act (Clinger-Cohen Act of 1996)*, Section E of the *National Defense Authorization Act for Fiscal Year 1996*, Public Law 104-106.

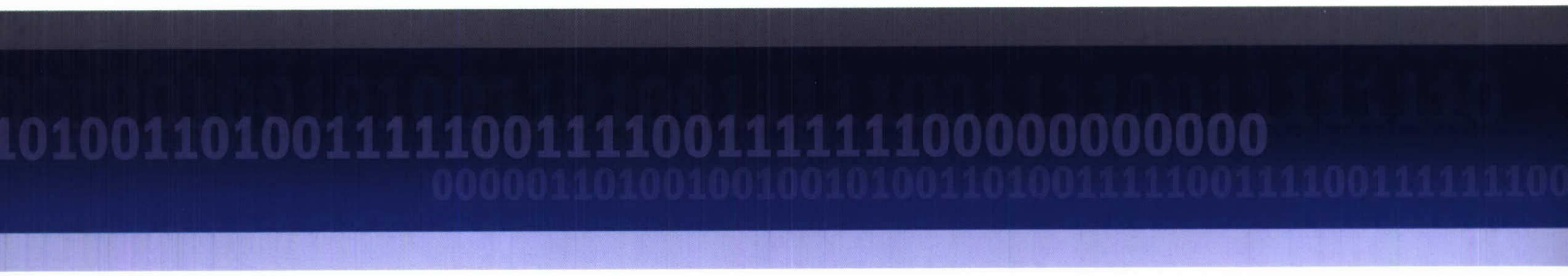
21. United States Department of Defense, *Information Technology Portfolio Management*, DoD Directive 8115.01, October 10, 2005.

22. United States Department of Defense, Chief Information Officer, *GIG Architecture* Version 2.0, May 5, 2003.

23. *Federal Information Security Management Act of 2002*, Title III of *E-Government Act of 2002*, Public Law 107, 347; 44 U.S.C. §3541 to §3549.

24. Department of Defense Business Transformation Agency, *2006 Annual Report to Congressional Defense Committees, Status of the Department of Defense's Business Transformation Efforts*, March 15, 2006

25. Department of Defense Business Transformation Agency, Enterprise Transition Plan *2006 Update*, Draft August 4, 2006



The Power of
INFORMATION
Access Share Collaborate

DoD Chief Information Officer
6000 Defense Pentagon
Room 3E172
Washington, DC 20301-6000
www.dod.mil/cio-nii