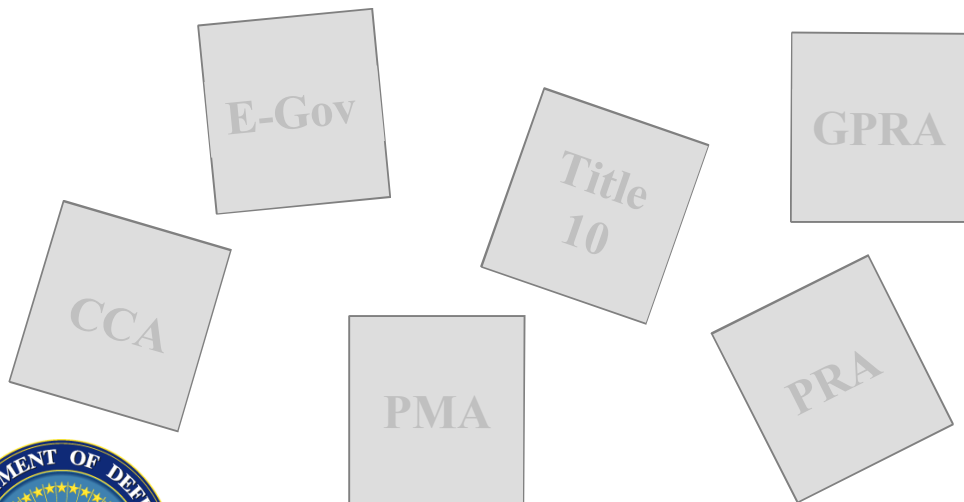


DoD Chief Information Officer Strategic Plan for Information Resources Management (IRM)



Power to the Edge ~~~~~

June 2004

Table of Contents

	Page
Foreword	iv
1.0. Introduction	1
2.0. President’s Management Agenda	2
3.0. Department of Defense Strategic Plan	3
4.0. Transforming Defense	4
5.0. Balanced Scorecard Approach	4
6.0. Transformation of DoD into the Information Age	7
6.1. Net-centricity Guiding Principles	9
6.2. Key Strategic Initiatives, Expected Outcomes and Challenges.....	10
6.2.1. IT Infrastructure.....	10
6.2.1.1. Transformational Communications Architecture.....	10
6.2.1.1.1. Global Information Grid Bandwidth Expansion	10
6.2.1.1.2. Installation Bandwidth Modernization	10
6.2.1.1.3. Joint Tactical Radio System.....	11
6.2.1.1.4. Advanced Wideband SATCOM	11
6.2.1.2. Internet Protocol Version 6	11
6.2.1.3. Commercial Off-the-Shelf Software (COTS)	11
6.2.1.4. Net-Centric Enterprise Services (NCES)	12
6.2.1.5. IT Infrastructure Outcome Goals	12
6.2.1.6. IT Infrastructure Challenges.....	12
6.2.2. Data/Information	12
6.2.2.1. Horizontal Fusion	12
6.2.2.2. Data/Information Management	12
6.2.2.3. Data/Information Outcome Goals	13
6.2.2.4. Data/Information Challenges	13
6.2.3. Processes and People.	13
6.2.3.1. Business Modernization	13
6.2.3.2. Train and Educate People	14
6.2.3.3. Processes and People Outcome Goals	15
6.2.3.4. Processes and People Challenges	15
6.2.4. Information Assurance	15
6.3. Experimentation, Pilots and Demonstrations	16
6.3.1. Rapid Acquisition Incentive (RAI)	17
6.3.2. Quantum Leap 1	17

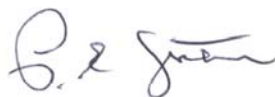
7.0. Governance	17
8.0. Expanded Electronic Government.....	19
9.0. Summary	20

Foreword

This Information Resources Management (IRM) Strategic Plan supports the statutory requirements of the Clinger-Cohen Act and related reform legislation, providing an information technology (IT) blueprint in support of the Secretary's transformation goals and the President's Management Agenda. This plan also provides the framework for the Department to manage its information resources and supporting technologies, to further transform DoD into the Information Age – depicting where we want to go and how we will get there strategically.

The destination is a global web-based (i.e., net-centric) environment where people fully utilize the network in which they have complete trust and confidence. End-user performance is not limited to the capabilities under direct command, but rather from the global reach of the network and all the capabilities that are connected by that network. This Plan is more than a discussion of initiatives that are being *considered*. It conveys those things that absolutely *must be done* and the *results* that must be achieved to ensure user-centric information sharing, information fusion, sense-making and decision-making in warfighting and business operations.

The goal of the Office of the DoD Chief Information Officer (CIO) is to create a secure, assured enterprise infrastructure to enable network-centric operations. Achieving net-centricity is, however, a mandate requiring Department-wide commitment from the most senior levels to the smallest organizational entities. Together we can achieve this transformational goal by forming strong partnerships, alliances, and communities of interest, all fully engaged in the way ahead.



Deputy DoD Chief Information Officer

1.0. INTRODUCTION

In 1996, the Information Technology Management Reform Act (ITMRA) was signed into law. This Act, together with the Federal Acquisition Reform Act, became known as the Clinger-Cohen Act (CCA). Coupled with other reform legislation such as the Paperwork Reduction Act (PRA) and the Government Performance and Results Act (GPRA), the CCA provides the statutory foundation for Federal Agencies to manage IT investments. Notwithstanding frequent use of the phrase “information technology,” the Act goes beyond IT and extends to the management of information resources – the management of the information itself and the technology that supports it.

Before applying IT, managers should examine their information processes and functions and determine whether: (a) the functions that IT will support are central to, or are priorities for the Department’s mission; and (b) the private sector or another government agency can perform the particular function more effectively at less cost. If the decision is made to retain the functional process in-house, it should be routinely and systematically benchmarked against models of excellence in the public and private sector. Benchmarks and associated analyses, as well as business reengineering practices and methodologies, should be used to develop, simplify, or refine functional processes before IT solutions are applied. Similar introspective considerations are called for in the President’s Management Agenda (PMA).

Information technology should be viewed as a tool that enables the Department to perform its mission and support functions effectively and efficiently. In essence, IT projects and their associated investments should:

- Support the DoD’s core mission, goals, objectives and priorities; show measurable improvements in mission performance; and align with mission-related outcomes;
- Be performance- and results-based; and
- Be consistent with the DoD enterprise architecture that integrates work processes and information flows with the technology to achieve the DoD mission.

This Information Resources Management Plan reflects the strong linkages among the CCA requirements, PMA, DoD Strategic Plan, DoD Chief Information Officer’s agenda, and the investments in information resources -- including IT, processes, and people. The PMA provides a strategy for improving the management of federal government resources, and reinforces the need for projects and their associated investments to be performance and results-based. The Quadrennial Defense Review (QDR) Report, “the DoD Strategic Plan,” outlines DoD goals, priorities, and strategies for the demands of the present, in addition to preparing for the future defense of the nation. Strategies for

managing information, and establishing performance outcomes and tracking results, are reflected in recent management initiative decisions. The DoD CIO has established the vision, goals, objectives, and guiding principles; and in partnership with others, is pursuing strategies and initiatives to further transform the Department into the Information Age. While there are varying degrees of risks that are associated with the pursuit of each of these, there are also tremendous opportunities. The challenges are to aggressively and systematically advance these opportunities in a collaborative way – keeping the customer in mind; undertaking solid approaches to manage and mitigate risks; and maintaining sound management principles as we proceed with transformation and introduce new ways of doing business.

2.0. PRESIDENT’S MANAGEMENT AGENDA (PMA)

	PMA	CCA
Management Reform Focus	Federal Government	IRM in the Federal Government
Guiding Principles	<ul style="list-style-type: none"> ▪ Performance -- and results-based ▪ Accountability ▪ Citizen-focused 	<ul style="list-style-type: none"> ▪ Performance -- and results-based ▪ Accountability ▪ Customer-focused

Figure 1 - PMA and CCA Context

The PMA may be viewed as having two components. One component includes five government-wide areas where the opportunity to improve performance is the greatest. Among these five areas are: strategic management of human capital, competitive sourcing, improved financial performance, expanded electronic government, and budget and performance integration.

The other component provides the context in which reform of the areas will occur, and reinforces the guiding principles of CCA with regard to improving IRM. Irrespective of whether the agency is DoD or a civil agency; or whether the project is IT, finance or another function, the same core management principles must be applied. The project and its associated investment should be tied to the mission, goals, objectives, and priorities of the organization; it should be performance-based and results-oriented; its proponents should be held accountable for the results; and it should be customer-focused. It is within the spirit and intent of these core management principles that the DoD is moving forward in the management of its information resources.

3.0. DEPARTMENT OF DEFENSE STRATEGIC PLAN

The DoD's IRM Plan is driven by the tenets of DoD's Strategic Plan, the Quadrennial Defense Review (QDR) Report. The DoD Strategic Plan is required by the Government Performance and Results Act, and serves as the overall planning document for the Department; the essence of this strategy is transformation. It provides the basis for identifying the Department's core missions, priorities, goals, and objectives; and how they will be achieved and measured. The current QDR, dated September 30, 2001, embodies a new defense strategy that serves the broad national objective of peace, freedom and prosperity. This strategy, which seeks to defend freedom for the United States and its allies and friends is based upon four defense policy goals:

- Assuring allies and friends of the United States' steadiness of purpose and its capability to fulfill its security commitments;
- Dissuading adversaries from undertaking programs or operations that could threaten U.S. interests, or those of our allies and friends;
- Deterring aggression and coercion by deploying forward the capacity to swiftly defeat attacks and impose severe penalties for aggression on an adversary's military capability and supporting infrastructure; and
- Decisively defeating any adversary if deterrence fails.

These goals are supported by an interconnected set of strategic tenets:

- Managing risk -- because resources are always finite, hard choices must be made that take into account a wider range of risks than was necessary in the past;
- A capabilities-based approach -- that focuses more on how an adversary might fight, rather than who the adversary might be and where a war might occur;
- Defending the United States and projecting U.S. military power;
- Strengthening alliances and partnerships, and security relations;
- Maintaining favorable regional balances -- to secure peace, extend freedom, assure allies and friends; and to convince potential adversaries that the benefits of hostile acts against the interest of the United States are far outweighed by their cost and consequences;
- Developing a broad portfolio of military capabilities -- to prevail over current challenges and to hedge against and dissuade future threats; and

- Transformation of the U.S. Military and Defense Establishment -- the heart of this new strategic approach.

4.0. TRANSFORMING DEFENSE

The Department's leadership recognizes that continuing "business as usual" is not a viable option given the new strategic era and the internal and external challenges facing the U.S. military. Without change, the current defense program will only become more expensive to maintain over time, and it will forfeit many of the opportunities available to the United States today. Without transformation, the U.S. military will not be prepared to meet emerging changes. At the same time, it would be imprudent to transform the entire force all at once. A balance must be struck between the need to meet current threats, while transforming the force over time. Therefore, the Department is committed to undertaking a sustained process – based on clear goals – and strengthening the spirit of innovation in its people, while remaining prepared to deal with extant threats.

5.0. BALANCED SCORECARD APPROACH

A Balanced Scorecard (BSC) approach is being used to manage the defense strategy, and balance the demands of the present, against preparation for the future, consistent with the strategy's priorities.

The BSC is a management tool that enables organizations to clarify their vision and strategy and translate them into action. It provides feedback around both the internal processes and external outcomes to continuously improve strategic performance and results.

If the centerpiece of the BSC is the defense strategy, its cornerstone is the risk management framework which consists of the following four dimensions:

- Force management – the ability to recruit, retain, train, and equip sufficient numbers of quality personnel and sustain the readiness of the force while accomplishing its many operational tasks;
- Operational – the ability to achieve military objectives in a near-term conflict or other contingency;
- Future challenges – the ability to invest in new capabilities and develop new operational concepts needed to dissuade or defeat mid- to long-term military challenges; and

- Institutional – the ability to develop management practices and controls that use resources efficiently and promote the effective operation of the Defense establishment.

FORCE MANAGEMENT RISK		OPERATIONAL RISK	
Maintain a Quality Workforce.	Ensure Sustainable Military Tempo. Maintain Workforce Satisfaction.	Do We Have the Forces Available?	Are They Currently Ready?
Maintain Reasonable Force Costs.	Shape the Force of the Future.	What are the Critical Needs, Systems, People, Sustainment, and Infrastructure?	Are We Prepared for Successful Strategy and Plan Execution?
INSTITUTIONAL RISK		FUTURE CHALLENGES RISK	
Streamline Decision Processes. Drive Financial Management and Acquisition Excellence.	Improve the Readiness and Quality of Key Facilities.	Drive Innovative Joint Operations (CONOPs, Experiments, Etc.).	Define Future Human Capital Skills and Competencies.
Manage Overhead / Indirect Cost.	Realign Support to the Warfighter (including Defense Agencies).	Develop More Effective Organizations.	Define and Develop Transformational Capabilities.

Figure 2 – Performance Outcome Goals

Departmental performance outcome goals (Figure 2) are associated with each of the four risk management areas. Initiatives to achieve these outcome goals include mitigating factors for the risk areas.

This framework is the basis for the DoD CIO and other Principal Staff Assistants to align their efforts with the defense strategy and to develop, within their sphere of responsibility, specific outcome goals, performance measures, and initiatives to mitigate risks associated with the above four areas. These are then cascaded down to the DoD Components and sub-components where supporting goals and metrics within their sphere are developed. As reflected in Figure 3, the entire process provides assurance that everyone is “singing from the same sheet of music” and the music sheet is what is important to the senior leadership and critical to the DoD mission, goals and priorities. It provides a focused, structured and disciplined way for every organization to:

- Align their initiatives with the next higher or lower organization and ensure that all organizations’ performance objectives are related to indicators of the Department’s performance at the highest levels;

- Have reasonable assurance that it is “doing the right things and doing things right;” and
- Maintain accountability.

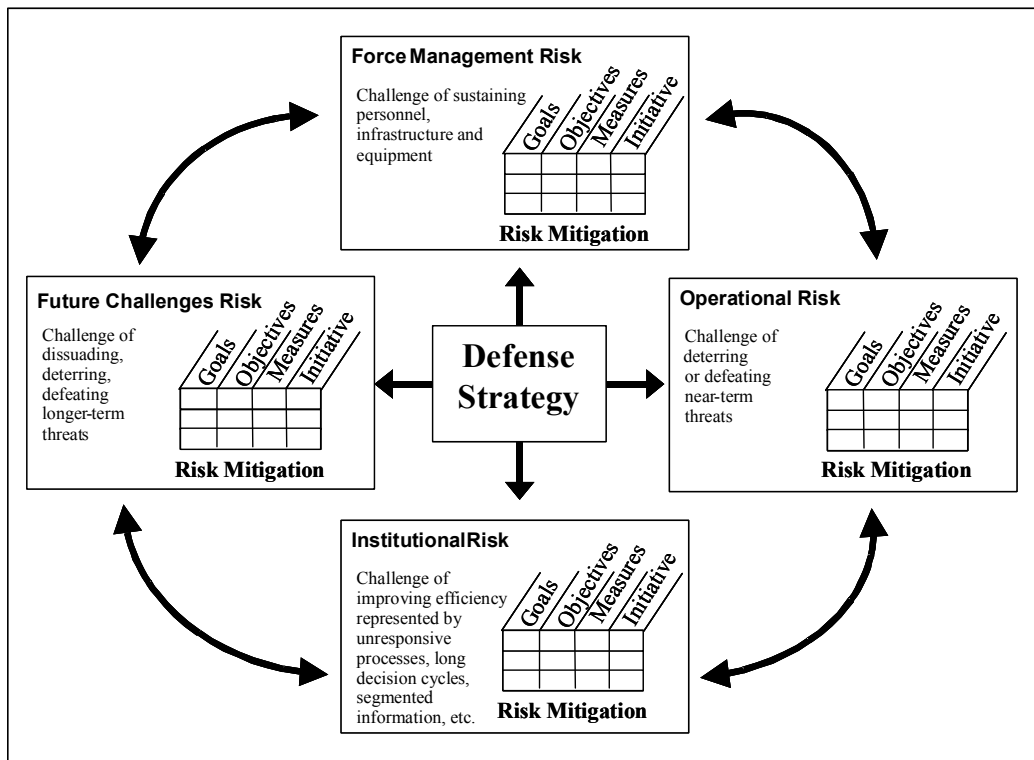


Figure 3 – Defense Balance Scorecard Approach
 (Adapted from “The Balanced Scorecard “ by Robert S. Kaplan and David P. Norton)

The DoD CIO is pursuing a strategy and a number of initiatives that will mitigate “operational and future challenges” risks, and support force readiness.

6.0. TRANSFORMATION OF DOD INTO THE INFORMATION AGE

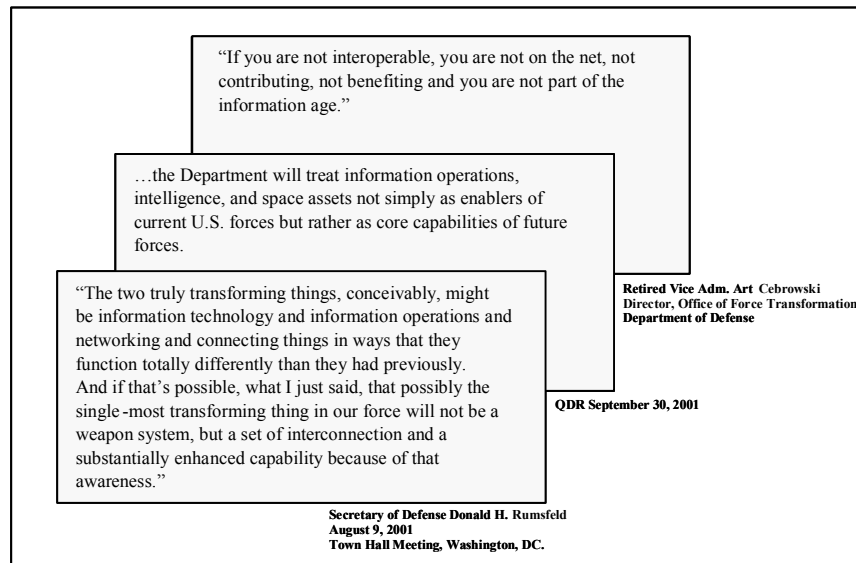


Figure 4 - View from the Top

“The United States is transitioning from an industrial age to an information age military. This transition requires transformation in warfighting and the way we organize to support the warfighter. Although the end-state of transformation cannot be fully defined in advance, we do know some of the necessary prerequisites for transformation. In particular, we know that early transformation requires exploiting information technology to reform defense business practices, and to create new combinations of capabilities, operating concepts, organizational relationships, and training regimes.”

The above quote from the Secretary’s Transformation Planning Guidance, dated April 2003, points to the fact that DoD is increasingly dependent upon information and decision superiority, and information technology. Of the six critical operational goals in the QDR that provide the focus of DoD’s transformational efforts, two specifically highlight and reflect this dependency:

- Assuring information systems in the face of attack and conducting effective information operations; and
- Leveraging information technology and innovative concepts to develop an interoperable, joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) architecture and capability that includes a tailorable joint operational picture.

The DoD CIO is providing leadership in achieving both of these goals. The DoD CIO serves as the Principal Staff Assistant (PSA) for DoD IRM matters, and is supported in this role by the Deputy CIO. In view of his overarching IRM responsibilities, the DoD CIO is enabling “the Information Age transformation of the DoD by building the foundation for achieving network-centric operations through policies, program oversight, resource allocation, and the provision of value-added support” to the warfighting and business communities.

The DoD CIO’s vision is to provide “Power to the Edge” by providing an environment where “*people throughout the trusted, dependable and ubiquitous network are empowered by their ability to access information and recognized for the inputs they provide.*” That is, the vision is to have an information environment where people fully utilize and trust the network; thus their performance is not limited by the capabilities that are under direct command, but enhanced by the global reach and all the capabilities that are interconnected by that network to provide the edge they need to prevail in any situation.

In support of this vision, the CIO has established the following goals:

- Make information available on a network that people depend on and trust;
- Populate the network with new, dynamic sources of information to enable defeating the enemy;
- Deny the enemy comparable advantages and exploit weaknesses; and
- Partner with the Chief Financial Officer (CFO), and provide support and oversight to the CFO’s initiatives to improve the efficiency of business processes.

Four overarching strategies provide the means to achieve these goals and provide a more focused approach and framework for the pursuit of initiatives, the development of policies and programs, investments in resources, and the measurement of progress and results. The four strategies are:

- *IT Infrastructure*: Achieve a ubiquitous, secure, robust network to enable greater information sharing and shared situational awareness.
- *Information/data*: Create an information/data management environment that assures user-centric information sharing, information fusion, sense-making and enables greater collaboration and enhanced situational awareness among a better-informed set of users.

- *Processes and People*: Influence and broker change in which data and information are generated, processed and used in warfighting and business operations; and educate and train individuals so they can understand, accept, embrace, as well as support and effectively participate in these changes.
- *Information Assurance*: Measures that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

6.1. Net-centricity Guiding Principles

Transformation into the Information Age is, indeed, a journey; and like any journey where there are many participants, it's not enough to know where we are and our destination. Collectively, we must understand the "rules of the road," or the core principles by which we all will be guided. It also helps to have a sense of why the principles are important. The following five key tenets are being employed to ensure effective and efficient transformation to net-centricity.

- *"Only handle information once (OHIO)."* Collecting information or replicating data entry is costly and adversely affects efficiency in both combat and business operations. "Only handling information once" requires that processes be re-engineered, and that technology and processes are integrated to minimize time and effort dedicated to data collection and entry.
- *"Post before processing"* means that access to data for disparate needs is not delayed by unnecessary processing. Users will have the technical capability to access all data when they want it and in the way they want it.
- Users will *"pull"* data as needed instead of having massive amounts of information *"pushed"* to them regularly, regardless of whether it is needed.
- *Collaboration technologies* will assist users in making sense of the data that is pulled. For example, subject matter experts from diverse units or organizations are frequently called upon to come together to make sense out of special situations. The ability to pull expertise from both within a unit, as well as from across the Department is a value-added feature of net-centricity.
- A *reliable* network is key to a net-centric environment. Diverse information pathways must be in place to achieve this reliability. Therefore, interoperability and information assurance must be the rule and not the exception.

6.2. Key Strategic Initiatives, Expected Outcomes and Challenges

The Department is undertaking a number of key initiatives that will fundamentally change the way we manage our information resources, the way we fight in the Information Age, and how we manage and assure the information resources that support the warfighters. Among these are: the Transformational Communications Architecture, Global Information Grid Bandwidth Expansion, Joint Tactical Radio System, Advanced Wideband SATCOM, Net-centric Enterprise Services, Horizontal Fusion, and Business Modernization, as well as investments in information assurance and people resources. Each of these, as well as other initiatives, will be briefly discussed in the context of the net-centricity strategic-focused areas – IT Infrastructure, Information/Data Management, Processes and People, and Information Assurance.

6.2.1. IT Infrastructure

6.2.1.1. Transformational Communications Architecture: The Transformational Communications Architecture defines the transport element of the Global Information Grid (GIG) and will be composed of three fully integrated segments. The terrestrial segment will be based upon fiber optics and include the GIG Bandwidth Expansion. The wireless or radio segment will be based upon the software programmable Joint Tactical Radio System. The space-based segment will be composed of several systems with the Advanced Wideband System serving as a gap-filler while we pursue the objective of Transformational Communications Satellite capability.

6.2.1.1.1. Global Information Grid (GIG) Bandwidth Expansion: Current telecommunication lines are not robust enough to handle the volume of information needed to facilitate optimum, strategic decision-making. The GIG Bandwidth Expansion (GIG-BE) will provide for the required robustness. It will use advanced fiber optical technology to upgrade telecommunications lines at DoD's critical installations, and provide networked services with unprecedented bandwidth to operating forces and operational support activities. The GIG-BE will provide approximately 100 times the current telecommunications capacity to critical Defense sites around the world. An increase in capacity of this magnitude will permit dual use of the bandwidth – with warfighting command, control, and intelligence functions as a primary mission and support activities as an auxiliary function.

6.2.1.1.2. Installation Bandwidth Modernization: Expansion of GIG Bandwidth will provide a solid foundation for DoD's net-centric transformation. However, base-or installation-level bandwidth also must be upgraded to guarantee connectivity and ensure maximum benefits are obtained from the GIG-BE initiative. Accordingly, appropriate DoD Components are developing installation bandwidth expansion strategies that will

provide a bridge from the installation- or base-level telecommunications infrastructure to the expanded GIG bandwidth.

6.2.1.1.3. Joint Tactical Radio System (JTRS): JTRS will be a family of software programmable, modular, multi-band, multi-mode, Internet Protocol (IP) based communications systems that will become the primary means of communications connectivity for warfighters during combined and coalition operations to include the digital battlefield environment. All waveforms, protocols, encryption, and communications processes, and hardware will be implemented around open standards architecture. The family of radios will be scaleable by virtue of form, fit, and cost will be expandable using an open software communications architecture (SCA) standard. The family will consist of three domains –airborne, ground, and maritime/fixed stations – and will initially include five radio family members to include handheld, man-packed, vehicular mounted, airborne and maritime/fixed station.

6.2.1.1.4. Advanced Wideband System (AWS)/Transformational Communications Satellite (TSAT): The space-based segment of the Transformational Communications Architecture is critical because many users are deployed in areas where optical fiber is unavailable, and many of our information sources, particularly intelligence, surveillance and reconnaissance capabilities, are airborne – making them especially difficult to link into a wideband network. The AWS will, in essence, extend the network's full capabilities to mobile and tactical users. The TSAT will expand AWS capabilities and incorporate Internet Protocol and laser communications capabilities into the Department's satellite communications constellation.

6.2.1.2. Internet Protocol (Version 6) (IPv6): Today, the Internet Protocol (IP) provides the foundation for interoperability across DoD's GIG; essentially, it enables the networking of nearly all space-based, terrestrial and radio communications. The Department must, however, transition to the next generation of the Internet Protocol, IPv6, to achieve a high performance, secure, end-to-end, net-centric environment, to accommodate a dramatically expanded and increasingly mobile set of network users; as well as network enabled sensors, weapon systems, and information technology systems and devices. The goal is to complete the transition to IPv6 by FY08 for all DoD networking. Some key elements of the transition are: (a) as of October 2003, all GIG assets developed, acquired or procured are required to be IPv6 capable in addition to being backward compatible with IPv4; and (b) significant segments of the DoD will transition to IPv6 beginning in FY05 and increasing through FY07. Pilot implementations will provide DoD with the knowledge and confidence to complete the transition.

6.2.1.3. Commercial Off-the-Shelf (COTS) Software: The reliability, trustworthiness, and utility of commercial technologies have grown tremendously in the last few years.

Like commercial businesses, the DoD is taking full advantage of this trend to support its enterprise goals. Specifically, we are promoting policies and establishing incentives designed to increase the use of COTS software across DoD. We are expanding the Enterprise Software Initiative to reduce cost by bulk/volume buying. The Department is also looking for opportunities to divest itself of its internal software design activities.

6.2.1.4. Net-Centric Enterprise Services (NCES): The NCES program will develop and provide a common set of computing, networking, and data services to support enterprise users. These capabilities and services will enable users to rapidly and precisely discover information; efficiently task information providers; post information holdings; and dynamically form collaborative groups for decision-making in a manner that can be customized to meet specific mission demands.

6.2.1.5. IT Infrastructure Outcome Goals: The expectation is that we will have an *IT infrastructure* where there are no technical limitations on the capability to access, retrieve, share, disseminate, or fuse information and data. The network is secure, dependable, and reliable with seamless connectivity and collaboration capabilities at all times across geographical, organizational, and mission boundaries. Further, the network has the capability to collect, process, disseminate, maintain, and protect an uninterrupted flow of information.

6.2.1.6. IT Infrastructure Challenges: The challenges are to identify IT infrastructure major risks early-on and develop mitigation plans; develop the right metrics to gauge value-added progress; and to synchronize IT infrastructure initiatives with other strategic area initiatives.

6.2.2. Data/Information

6.2.2.1. Horizontal Fusion: Networks are essential to a net-centric environment, but they have limited value without quality data that are reliable, accessible and usable in an integrated manner. The Horizontal Fusion initiative will provide tools and means that integrate the smart “pull” of data with expert interpretations of the information. It is aimed at providing the tools that allow users to identify what data is available, access it, smartly pull and fuse it, and make sense of the data gathered. These tools will require investing in data content and management, as well as the acquisition of commercial applications. Although the initial focus is on Intelligence, lessons learned from the intelligence community will be exported to and employed by the business communities such as finance, logistics, and personnel.

6.2.2.2. Data/Information Management: Computers and communications networks process, transport, and deliver data. Horizontal fusion tools provide the means to search

for, pull and fuse data from a myriad of sources, and allow users to make sense of data. What about the most basic entity – the data itself? In essence, information is purposefully constructed from data; knowledge is discovered with the understanding of information; and decision support is the appropriate application of data, information, or knowledge to meet mission or policy objectives. Clearly, the crux of it all is “the data” – its visibility, accessibility, trustworthiness, and understandability. Arguably, the success of net-centricity is based largely on our ability to effectively manage the data. Accordingly, the DoD Net-Centric Data Strategy has evolved with several features that we will promote and implement. For example, it emphasizes the use of catalogs, and “search” services so users can discover the existence of data with or without prior knowledge of its existence, and registries with data formats and structures to ensure discovered data is understandable and usable. It also addresses the means by which data is posted, tagged, advertised, shared, and governed, as well as methods that facilitate trust in the data.

6.2.2.3. Data/Information Outcome Goals: The expectation is that we will have a *data/information* environment where every data element is posted and its structure and content is maintained by an authoritative source; data is available to the people that want it, the way they want it, and when they want it – except when limited by policy, regulation, or security; people depend on and trust the data; and data is protected, secure, and resilient against information warfare, terrorist, and criminal activities.

6.2.2.4. Data/Information Challenges: The challenges are to identify data/information major risks early-on and develop mitigation plans; develop the right metrics to gauge value-added progress; and to synchronize data/information initiatives with other strategic area initiatives.

6.2.3. Processes and People

6.2.3.1. Business Modernization: “Improved Financial Performance” is one of five Government-wide initiatives in the PMA. Among other things, the initiative is expected to result in financial systems that routinely produce information that is timely, useful, and reliable. Three years ago, the Under Secretary of Defense (Comptroller)/Chief Financial Officer (USD(C)/CFO) established the Business Management Modernization Program (BMMP). Under the leadership of the USD(C)/CFO, and in partnership with the DoD CIO and the DoD business communities, the DoD is moving toward the USD(C)’s vision: “the Department will be managed in an efficient, business-like manner in which accurate, reliable and timely financial information, affirmed by clean audit opinions, is available on a routine basis to support informed decision-making at all levels throughout the DoD.”

Notwithstanding the apparent emphasis on “finance,” the Program encompasses all business areas – finance and accounting, logistics, acquisition, human resources management, strategic planning and budgeting, and installation and environment; it is the vehicle through which USD(C)/CFO is driving the modernization of DoD business processes and systems. The BMMP scope is reflected in the Business Enterprise Architecture (BEA); it is the business component of the GIG Architecture, and provides the basis for business area communities to develop and/or refine their respective architectures (i.e., components of the BEA) and transform their business areas accordingly. The BMMP is, in effect, our e-business strategy.

While the USD(C)/CFO is leading this effort, a program of this magnitude, scope, and complexity requires the commitment and involvement of virtually every community of interest in DoD. The CIO community’s involvement includes providing support and oversight, and ensuring efficient and effective information systems are developed that will provide accurate, reliable, and timely performance and financial data; assessing architecture products for compliance with the GIG architecture; promoting business process improvements and ensuring that net-centric architectural tenets are reflected in these improvements; and providing for an enterprise information environment ensuring that its capabilities are synchronized with the business functions’ requirements.

6.2.3.2. Train and Educate People: Simply put – people are the “edge” in “Power to the Edge.” They are the “committed” providers and consumers of data and information, and the ones who must make sense of it. Moreover, they are the “committed” program managers who must acquire IT within cost, schedule and performance goals. They are the “committed” partners, stakeholders, and beneficiaries of what a net-centric environment offers. A thorough understanding, however, is a prerequisite for commitment. We must promote and build this understanding. We must have a concerted, orchestrated, concentrated, and sustained campaign of awareness to get people on board, educate and train them, define roles and responsibilities, and break down artificial barriers that make no sense in an Information Age. Taking these steps will minimize confusion and skepticism, and ensure that we all are working toward the net-centricity vision and goals from the highest levels on down to effectively and efficiently manage our information resources.

Sound, focused, and communicated strategic and business planning is a first step. Forums such as the DoD CIO Executive Board and the CIO World-Wide Conference offer good opportunities for getting the word out, and discussing issues and resolving them in a way that is in the best interest of the enterprise.

With respect to education and training, the DoD CIO has made it a top priority and is pursuing initiatives to educate and train managers, and to sustain a core of well-trained, highly qualified DoD IT and Information Assurance (IA) professionals. For example, the

Clinger-Cohen Competencies are being used as the foundation to identify IT management skills, knowledge and education requirements; competency requirements for the Federal Enterprise Architects are being used for curricula development; and IT training is being enhanced through classroom, web-based, and distributed learning initiatives.

The Information Resources Management College of the National Defense University has been designated as the primary source of IT management education and training for senior and mid-level managers. The College will continue to develop and/or maintain an array of programs (e.g., CIO Certificate Program, IA Certificate Program, E-Government Leadership) to meet the educational requirements of DoD managers and IT professionals.

The DoD Information Assurance Scholarship Program has been established to help meet the recruiting and professional development requirements of the DoD IT/IA workforce. A growing number of college students have received financial support to complete baccalaureate, masters or doctoral programs of study – increasing the quality and quantity of new entrants into the IA/IT fields within DoD and providing significant retention incentive for current DoD IT civilian and military personnel.

6.2.3.3. Processes and People Outcome Goals: People understand, accept, embrace, as well as support and effectively participate in the net-centric transformation. Champions exist throughout DoD, as well as in Congress and OMB. Processes are reengineered and reflect the net-centric architectural tenets. The Department has a core of well trained, highly qualified IT and Information Assurance professionals who can accept, anticipate, and generate the changes that a net-centric environment will enable.

6.2.3.4. Processes and People Challenges: The challenges are to identify process and people major risks early-on; develop mitigation plans and the right metrics to gauge value-added progress; and to synchronize processes and people initiatives with other strategic area initiatives.

6.2.4. Information Assurance

Trust and confidence in our information is paramount for net-centric operations. None of our critical systems, networks, platforms, or sensors should be developed and deployed without the necessary security and interoperability capabilities to make them “net-ready.” As such, the information assurance community has developed five key strategy priorities or goals to achieve the vision of the Department’s senior leadership. These priorities are being co-developed with core IT initiatives, programs and architectures to ensure information assurance is integrated throughout the IT infrastructure and services, and serve as the primary tenets for the provision of “trust” and confidence in DoD’s information. The five priorities address: (1) protecting information; (2) defending

systems and networks; (3) providing integrated IA situational awareness for improved network command and control; (4) transforming and enabling IA capabilities; and (5) creating a professional IA empowered workforce.

6.3. Experimentation, Pilots and Demonstrations

Many of the net-centricity concepts are a dramatic departure from the way the Department acquires, manages, and uses its information resources today. Figure 5 provides a brief description of what concepts will prevail in the future (i.e., IN) and those that will fall by the wayside (i.e., OUT).

What's In? What's Out? with Net-Centricity	
<u>IN</u>	<u>OUT</u>
<ul style="list-style-type: none"> • Situational Awareness • Self-synchronizing ops • Information pull • Collaboration • Communities of Interest • Task, post, process, use • Only handle information once • Shared data • Persistent, continuous IA • Bandwidth on demand • IP-based Transport • Diverse routing • Enterprise Services • COTS-based, net-centric capabilities 	<ul style="list-style-type: none"> • Limited operational picture • Autonomous ops • Broadcast information push • Individual • Stovepipes • Task, process, exploit, disseminate • Multiple data calls, data duplication • Private data • Perimeter, one-time security • Bandwidth limitations • Circuit-based Transport • Single points of failure • Separate infrastructures • Customized, platform centric IT

Figure 5 – What's In? What's Out?

We recognize that some of these new and innovative concepts of the future have not been tested for their operational viability, and the details of implementation have yet to be worked out. Experimentation and pilots, as required, are ways in which the DoD intends to better understand the net-centricity issues and pitfalls, and work out the details before deploying some of these capabilities. However, these efforts must be structured to produce results; they should be: (a) clearly defined, scoped, and documented; (b) designed and focused to test a clearly defined set of hypotheses under controlled and unbiased conditions; (c) professionally conducted to include the manner in which data is collected, analyzed, and measured; (d) designed to have a beginning and an end; and (e) programmed with a clear path for implementation, if successful. Following are two examples of pilots and experiments that are underway.

6.3.1. Rapid Acquisition Incentive – Net Centricity (RAI-NC): This initiative has been established to encourage the acceleration of IT projects in support of net-centric business transformation and the implementation of the President’s Management Agenda. It provides opportunities for DoD Components at all levels to bring forth promising IT projects to be piloted that will: (a) support the advancement of net-centric tenets and transformational processes; (b) field business case-driven, proof-of-concept pilot projects; and (c) provide pilot project results capable of being exported across the DoD. The FY04 RAI-NC Portfolio consists of four pilots. Results of the FY04 pilot projects will be collected and analyzed for broader use within the Department.

6.3.2. Quantum Leap-1 (QL-1): QL-1 is the FY03 Horizontal Fusion Portfolio demonstration of net-centric capabilities available via a portal. QL-1 goals are to: (a) increase availability of information critical to combat decision making; (b) augment collaborative command and control processes; (c) substantially improve situational awareness; (d) reduce decision-making cycle time; (e) demonstrate simultaneous analysis of the same data by different users in disparate locations; and (f) measure, analyze, and validate results for improvements in data reliability, portal availability, and adaptability, and responsiveness. The FY03 Portfolio demonstrated that net-centric operations are feasible today. The FY04 Portfolio continues these demonstrations, further refining and the launching of new initiatives to pilot cross-domain information sharing, secure wireless, and additional infrastructure solutions. The FY04 Portfolio consists of 14 initiatives with a combination of high and low-risk tolerance levels. Initiatives that are unable to achieve identified net-centric goals are dropped from the portfolio. Initiatives are in the portfolio for a limited duration; the average time span is two years.

7.0. GOVERNANCE

Governance may be viewed in the context of strategic planning, policies, and forums for governing. Plans provide the vision, goals and objectives, and hopefully make sense out of what might otherwise appear to be diverse and random activities -- much like the intent of this Plan. Policies, including standards, are the regulations, as well as the uniform criteria, methods, processes and practices that guide our activities; for example, directives, instructions, and architectures. Governance forums bring in the people, oversight, control and evaluation dimension; for example, the Defense Resources Board (DRB), Defense Acquisition Board (DAB), Joint Capabilities Integration and Development System (JCIDS), and the DoD CIO Executive Board. We are considering each of these views as we create and/or refine our net-centric governance processes. We will:

- Emphasize strategic and business planning;

- Leverage existing DoD key decision support systems (i.e., JCIDS, PPBE, DAB) to the maximum extent possible;
- Have governance processes that are nested, but clearly integrated, to include being integrated with the key decision support systems;
- Develop new policies and standards, if necessary; but first we must analyze existing ones, and retain, modify or cancel them depending on the value they add to our future environment;
- Design net-centric concepts into our operations, systems, technical activities, reflect these in our architectures; and use these architectures as a means to guide and manage IT investments;
- Take a portfolio approach to managing and overseeing IT investments. As envisioned, this approach will allow portfolio managers to assess the tradeoffs among competing investment opportunities in terms of their benefits, cost and risks, and make investment decisions based on a better understanding of what will be gained or lost through the inclusion or exclusion of a particular investment. Under this approach, IT investments are grouped and managed as portfolios linked to mission areas or domains that are being supported by the IT project. Currently, we have six domains in the business mission area (i.e., Finance and Accounting, Acquisition, Human Resource Management, Installation and Environment, Logistics and Strategic Planning and Budget); and three domains in the enterprise information environment mission area (i.e., Communications, Computing, and Core Enterprise Services). The Chairman of the Joint Chief of Staff is identifying the warfighting mission area domains.

A BSC approach will be used to manage the net-centricity strategy, align the initiatives with the new defense strategy, and ensure that programs remain on track. A recent management initiative decision to establish performance outcomes and track performance results is the point of departure. This decision aligns the Department's performance management activities with the PMA, the Annual Defense Report, and the risk management framework established in the QDR.

The "net" effect is that net-centric initiatives with specified goals, objectives, outcomes, and metrics are aligned with the CIO goals, DoD outcome goals, risk factors, and the new defense strategy, as well as the PMA.

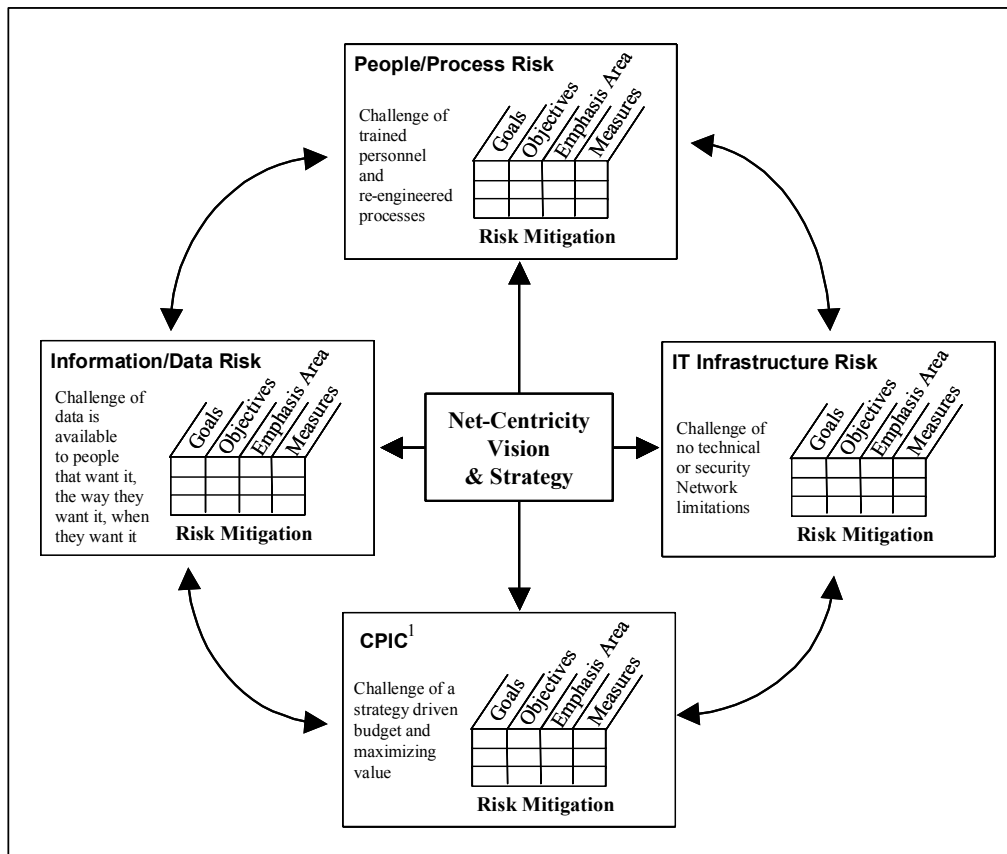


Figure 6 – Net Centrality Balanced Scorecard

At the other end of the spectrum, the CIO goals are cascaded down to the DoD Components and sub-components, which will be expected to develop supporting initiatives. Work groups, comprised of the DCIO staff and Components, have been formed to address the strategic emphasis areas and initiatives. These groups periodically report to the DCIO and the DoD CIO Executive Board on their progress. The entire process aligns each organization's initiatives with the next higher or lower organization and ensures all organizations' performance objectives are related to indicators of the Department's performance at the highest levels.

8.0. EXPANDED ELECTRONIC GOVERNMENT

This is a key Government-wide initiative in the PMA. As reflected throughout this document, the Department is committed to, and involved in, expanding the use of IT in mission and business functions. While transforming the Department into the Information Age, the initiatives described in this plan will, at the same time, address the six chronic problems, as described in the PMA, that limit results from Federal IT spending – paving

¹ CPIC - Capital Planning and Investment Control

cow paths, redundant buying, inadequate program management, poor modernization blueprints, islands of automation, and poor security. We will continue to convey progress on and the results of our initiatives in areas such as IT program management and performance, DoD participation in multi-agency efforts, enterprise architecture, IT security, and the expansion of business cases.

9.0. SUMMARY

This is the DoD CIO's Strategic Plan for information resources management to achieve a net-centric environment. Are there challenges and risks? Yes; no effort as important and complex as this one is void of challenges and risks. Will there be instances of dashed hopes? Yes; but there will also be many short-, mid- and long-term successes. Will there be some restructuring and re-direction? Yes; particularly in the data/information area because some of these concepts are experimental research and development. Will the targeted environment be created in short order? Absolutely not; it will take years, but we have mechanisms that will keep us focused, disciplined, and accountable with an eye toward the vision and our ultimate customer – the warfighter. Notwithstanding the complexity, magnitude and risks, we are “doing the right things.” Moreover, we are putting structures and processes in place to “do things right,” and make good on the promises reflected herein.

*“Government likes to begin things – to declare grand new programs and causes and national objectives. But good beginnings are not the measure of success. **What matters in the end is completion. Performance. Results. Not just making promises, but making good on promises.** In my administration, that will be the standard from the farthest regional office of government to the highest office of the land.”*

Governor George W. Bush