United States Government Accountability Office

GAO

Report to Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Committee on Armed Services, House of Representatives

July 2004

DEFENSE ACQUISITIONS

The Global Information Grid and Challenges Facing Its Implementation

GAO-04-858

July 2004

DEFENSE ACQUISITIONS

The Global Information Grid and Challenges Facing Its Implementation

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-858, a report to Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Committee on Armed Services, House of Representatives

Why GAO Did This Study

The Department of Defense (DOD) is in the midst of transforming military capabilities. The transformation relies in part on the Global Information Grid (GIG), which is focused on building a new Internet-like network capability that DOD envisions will enable weapons and other systems and people to share information quickly, allowing warfighters to identify threats more effectively and to respond with greater precision and lethality. DOD plans to spend at least $21 billion through 2010 to build a core GIG capability. GAO was asked (1) to describe the GIG, including the concept, key acquisitions, and implementation and (2) to identify significant challenges facing DOD in implementing the GIG.

What GAO Recommends

GAO is not making recommendations in this report as this effort is focused on providing an initial overview of the GIG and challenges. Our future work will continue to assess how DOD is addressing challenges and the progress of key acquisitions. DOD-provided technical comments on this report are incorporated where appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-04-858.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert E. Levin at (202) 512-4841 or levinr@gao.gov.

What GAO Found

The GIG is a huge and complex undertaking that is intended to integrate virtually all of DOD's information systems, services, and applications into one seamless, reliable, and secure network. DOD's overall concept is to enable data access for a variety of systems and users in the network no matter which military service owns a weapon system or where a user might be located around the world. DOD is looking to the GIG to form the basis of a network-centric or "netcentric" way of fighting wars and to create a decisive advantage over adversaries. DOD has taken the following two-pronged approach to building the GIG:

(1) Invest in key acquisitions to build a core networking capability, including new communication satellites, next-generation interoperable radios, a new ground-based communication network with significantly expanded bandwidth, and services and applications to manage and protect the network and help users locate, post, and share information.
(2) Integrate other existing and planned weapon systems, information technology systems, and logistics, personnel, and other business-related systems into the GIG. To integrate other systems, DOD officials who created the concept for the GIG have developed an initial blueprint or architecture for the GIG and policies to formalize the GIG, and they are attempting to influence key acquisition and budgeting decisions to align investments and systems with the GIG.

The most critical challenge ahead for DOD is making the GIG a reality. While DOD has taken steps to define its vision and objectives for the GIG on paper and in policy and is beginning to make a heavy investment in the GIG as well as systems that will be heavily dependent on the GIG, it is not fully known how DOD will meet these objectives. For example, it is not known which investments should take priority over others and how these decisions will be enforced. Moreover, it is not known how DOD will assess the overall progress of the GIG and determine whether the network as a whole is providing a worthwhile return on investment, particularly in terms of enhancing and even transforming military operations. According to DOD officials, the enhancements DOD is making to its planning and budgeting processes are meant to begin addressing these questions. Until DOD implements an investment and oversight strategy for the GIG as a whole, it is at risk of making investments that do not fit DOD's vision for the future.

Highlights of Key Challenges Facing DOD's Implementation of the GIG

- Deciding what capabilities are affordable, what capabilities are unaffordable or not in line with DOD's vision for the GIG, and enforcing these decisions
- Assuring management attention and oversight are provided to assess the overall progress and return on investment
- Developing a trustworthy network so data owners will share data with a broader audience
- Advancing technologies on schedule
- Developing the means to protect the network and its data

Source: GAO analysis.

Contents

Tables

Figure

Abbreviations

DOD	Department of Defense
GIG	Global Information Grid
GIG-BE	Global Information Grid Bandwidth Expansion
IPv6	Internet Protocol Version 6
JTRS	Joint Tactical Radio System
NCES	Network Centric Enterprise Services
TSAT	Transformational Satellite
WIN-T	Warfighter Information Network-Tactical

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 28, 2004

The Honorable Jim Saxton
Chairman
The Honorable Martin T. Meehan
Ranking Member
Subcommittee on Terrorism,
Unconventional Threats, and Capabilities
Committee on Armed Services
House of Representatives

To achieve long-term dominance over evolving, sophisticated threats, the Department of Defense (DOD) is seeking to make transformational improvements to military capabilities. The transformation involves achieving information and decision superiority over adversaries, striking with precision, deploying and sustaining military power rapidly, and dominating the "battlespace" on land, at sea, in the air, and in space. DOD has said that a successful transformation hinges largely on disparate weapon systems sharing information seamlessly, regardless of which military service owns the system and preempting the need to retrofit weapon systems to solve compatibility issues with other systems in the field. Beyond the need to build new weapon systems according to a predetermined architecture, DOD says the transformation encompasses new doctrine and institutional changes for DOD and its partners.

One of DOD's key initiatives to respond to this transformation is the Global Information Grid (GIG). The GIG represents a collection of programs and initiatives aimed at building a secure network and set of information capabilities modeled after the Internet. The GIG is expected to facilitate DOD's transformation by allowing warfighters, policy makers, and support personnel to engage in rapid decision making. By having the ability to access and exchange information quickly, reliably, and securely through linked systems and military components, DOD believes that commanders would identify threats more effectively, make informed decisions, and respond with greater precision and lethality.

DOD began investing in the GIG in the late 1990s and plans to begin fielding a core capability by about 2010. It plans to spend at least $21 billion to develop the GIG through fiscal year 2010. Full implementation of the GIG would occur in the 2020 time frame. Given the GIG's overall investment and importance to DOD, as well as a lack of clarity about what

the GIG entails, you requested that we review DOD's strategy for developing and deploying the GIG. As agreed with your office, our work initially focused on (1) describing the GIG, including the overall concept, key acquisitions, and implementation strategies and (2) identifying challenges facing DOD's implementation of the GIG. Subsequent efforts will further explore the challenges we have identified and the progress of key acquisitions.

Objectives, Scope, and Methodology

To gain a better understanding of the overall concept, key acquisitions, and implementation strategy, we reviewed relevant DOD plans, policies, guidance, and other documents pertaining to the GIG. We also reviewed briefings prepared for high-ranking DOD officials and other organizations within the department to obtain more up-to-date information on the status of GIG activities and costs of key components. Funding and cost information was obtained from budget exhibits and other accounting reports compiled by the DOD. We did not conduct a comprehensive review of the financial reports or records. Also, we did not evaluate the content and quality of the GIG architecture and standards. In addition, we interviewed key officials responsible for the GIG in the Office of the Assistant Secretary of Defense for Networks Information and Integration (DOD's Chief Information Officer); the Defense Information Systems Agency; Office of the Under Secretary of Defense (Comptroller); Office of Program Analysis and Evaluation; Office of the Under Secretary of Defense for Acquisition, Technology and Logistics; and Office of the Joint Chiefs of Staff. We held interviews with officials representing the Offices of the Chief Information Officer for the Air Force, Army, Navy, and U.S. Marine Corps.

To identify the challenges associated with GIG implementation, we examined studies, reports, and guides on the GIG; DOD's effort to transition toward more network-based military operations; and DOD's efforts to enhance its capability to acquire joint systems that were completed by DOD, the Defense Science Board, and other research entities, such as the Center for Strategic and International Studies. We examined reports and guides completed by the Congressional Research Service, Congressional Budget Office, and GAO on managing technology projects, architectures, and information technology investments. We held interviews with previously identified DOD officials to discuss key challenges associated with the development and implementation of the GIG.

We performed our work from November 2003 to June 2004 in accordance with generally accepted government auditing standards.

Results in Brief

The GIG is a huge and complex undertaking that is intended to integrate virtually all of DOD's information systems, services, applications, and data into one seamless, reliable, and secure network. A primary difference between the GIG initiative and previous efforts is that it focuses on promoting interoperability by building an Internet-like network for DOD-related operations based on common standards and protocols rather than on trying to establish interoperability after individual systems and platforms have been fielded. DOD envisions that this type of network would not just ensure systems can easily and quickly exchange data, but also would change how military operations are planned and executed since much more information would be dynamically available to users.

DOD's plans for realizing the GIG involve building a new core network and information capability and successfully integrating the majority of its weapon systems, command, control, and communications systems, and business systems with the new network. The effort to build the GIG will require DOD to make a substantial investment in a new set of core enterprise programs and initiatives in order to develop and deploy new satellites capable of quickly transmitting and routing larger volumes of data, increased bandwidth capacity on the ground, new types of communications systems to be embedded on weapon systems, and new computer applications and services to enable information to be transferred globally. To integrate systems into the GIG, DOD has developed an initial blueprint or architecture for the GIG, developed new policies, guidance, and standards to guide implementation, undertaken proactive efforts to "market" the GIG and its potential benefits among various elements of DOD, and is attempting to influence key acquisition and budgeting decisions to align with the GIG. Depending on the extent DOD decides to rely on the GIG to facilitate military operations, the initiative could affect the way weapon systems and information technology systems are selected and built as well as how DOD military and civilian personnel collect, analyze, and share data.

The most critical challenge ahead for DOD is making the GIG a reality. While DOD has taken steps to define its vision and objectives for the GIG on paper and in policy and is beginning to make a substantial investment in the GIG as well as in systems that will be heavily dependent on the GIG, it is not fully known how DOD will meet these objectives. For example, it is not known which investments should take priority over others and how

these decisions will be enforced. Moreover, it is not known how DOD will assess the overall progress of the GIG and determine whether the network as a whole is providing a worthwhile return on investment, particularly in terms of enhancing and even transforming military operations. Until DOD implements an investment and oversight strategy for the GIG as a whole, it is at risk of making investments that do not fit its vision for the future. In addition, DOD faces risks inherent with the nature and scope of the effort it is undertaking, for example, risks related to protecting data within the thousands of systems that will be integrated into the network. Furthermore, the technical challenges to develop new networking and network management capabilities to support mobile, integrated communications are considerable. DOD recognizes these challenges, and many of the actions it is taking to implement the GIG are meant to address them. However, it is too early to assess how successful DOD will be in addressing the challenges and overcoming long-standing organizational impediments.

Description of the GIG

For the past two decades, DOD has been seeking solutions to improve interoperability and information sharing across its business and warfighting operations. Too often weapon and information technology systems have been acquired by the military services and defense agencies without regard for their ability to work in a joint operational environment.[1] As a result, extra layers of redundancy and common systems have been put in place to support military operations, but without the ability to easily and quickly exchange data.

DOD defines the GIG as a "globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information." The GIG is meant to improve interoperability among DOD's many information systems and weapon systems. More important, the GIG is to facilitate DOD's effort to transform to a more network-based, or "netcentric," way of fighting wars and achieving information superiority over adversaries, much the same way as the Internet has transformed industry and society on a global scale. Netcentric operations and warfare, according to DOD, are the combination of tactics, techniques, and procedures that a networked force can employ to create a decisive

[1] U.S. General Accounting Office, *Joint Warfighting: Attacking Time-Critical Targets*, GAO-02-204R (Washington, D.C.: Nov. 30, 2001).

warfighting advantage. The GIG's role is to create an environment in which users can access data on demand at any location without having to rely on (and wait for) organizations in charge of data collection to process and disseminate the information. Data could emanate from a variety of sources, including weapon systems belonging to other military services, space-based intelligence, surveillance, and reconnaissance satellites, and DOD logistics, financial, and other systems that carry out business operations. Ultimately, DOD expects that most of these systems will become part of the GIG.[2]

With greater data access and a more robust communications infrastructure, DOD expects the GIG to enable more timely execution of military operations, collaborative mission planning and execution, common views of the battlespace, and more timely assessments of the condition of equipment and the levels of supplies. For example, according to DOD officials, greater information sharing could dramatically increase capabilities to rapidly identify and strike time-critical targets, such as mobile surface-to-air missile sites. In the past, such targets have proved to be elusive because the enemy is able to move them to safety in a shorter time frame than it takes U.S. military forces to detect, assess, and attack the targets. By having greater command of a battle situation, DOD expects that lethality and survivability of equipment and personnel would be increased. Armor protection could be scaled down in favor of more agility. In addition, the GIG would reduce the substantial resources and logistics needed to bring command, control, and communications systems to the war-fighting environment. Table 1 illustrates how DOD envisions the GIG will help transform military operations.

[2] DOD defines the GIG to include "all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority."

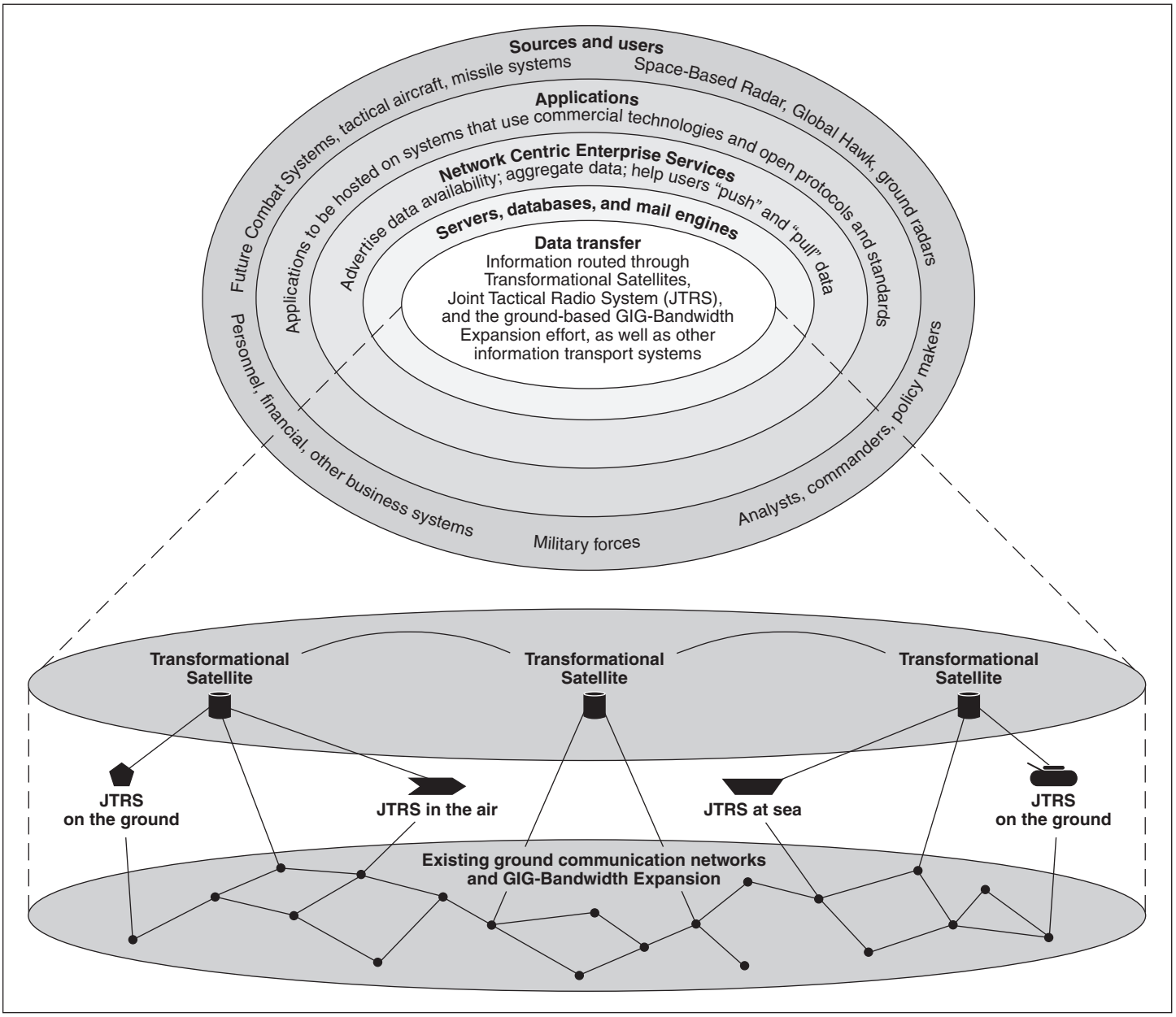
Table 1: How DOD Envisions GIG Will Help Transform Military Operations

Current	Future
Customized, platform-centric information technology	Network-centric, commercial off-the-shelf software, Web-based
Circuit-based transmission of data	Internet protocol-based transmission of data
Bandwidth limitations	Bandwidth on demand
Limited operational picture	Situational awareness
Fixed and remote command and control	Mobile, deployable, in-transit command and control
Broadcast (push) information to users	Post information on network and facilitate "smart" pull by users
Collect, process, exploit, disseminate	Collect, post, process, use
Individual	Collaborative
Stovepipe decision making	Communities of interest
Multiple data calls, data duplication	Handle information only once
Private data	Shared data
Perimeter, one-time security	Persistent, continuous information assurance
Single points of failure	Diverse routing
Separate infrastructures	Enterprise services
Interoperability by standard applications	Interoperability designed from start ("born joint")

Sources: DOD (data); GAO (presentation).

The GIG is to be much like the Internet, but with less dependence on ground-based and fixed systems and equipment to transmit and route data and more dependence on space-based and mobile, ad hoc systems to carry out these functions. Figure 1 shows the various layers of the GIG's overall concept. At the core are communications satellites, next-generation radios, and an installations-based network with significantly expanded bandwidth. These will provide the basic infrastructure through which data will be routed and shared. In addition, the GIG would employ a variety of information technology services and applications to manage the flow of information and ensure the network is reliable and secure. Various information technology tools would be available to help users determine what information is available, where to find it, and how best to use it. DOD envisions that communities of interest would be developed, linking users with common interests who would collaborate on analyzing and sharing information. Ultimately, most of DOD's sensors, weapon systems, business systems, and systems belonging to decision makers, military units, and allies would be tied into the GIG network—serving as both users and providers of data.

Figure 1: A General Depiction of DOD's Characterization of the GIG



Sources: DOD (data); GAO (analysis).

Acquisitions

DOD has taken a two-pronged approach to build the GIG: (1) invest in a set of core enterprise programs and initiatives to build a core network and information capability and (2) bring other existing and planned weapon systems, command, control, and communications systems, information technology systems, and logistics, personnel, and other business-related systems into the GIG network. The core network acquisitions are to be developed incrementally over time, with the aim of fielding the first increment of the GIG by 2010. The GIG is primarily being developed under the leadership and direction of DOD's Office of the Assistant Secretary of Defense for Networks and Information Integration in coordination with other components in the Office of the Secretary of Defense and Joint Staff. The Defense Information Systems Agency, military services, combatant commands, and other defense agencies also play roles in implementing the GIG. In addition, DOD's Strategic Command has responsibilities for eventually operating the GIG. Table 2 shows the key acquisitions for the GIG's core network and examples of additional acquisitions that must be integrated with the GIG.

Table 2: DOD Acquisitions Related to the GIG

Key acquisitions to build GIG's core network and information capability	Examples of acquisitions that must be integrated with the GIG
Communications satellites	Weapon systems
Interoperable radio systems	Sensors
Expanded bandwidth on the ground	Command, control, and communications systems
Information technology applications to support the network	Logistics, personnel, and other business-related systems

Sources: DOD (data); GAO (analysis).

Core GIG Network Acquisitions

According to DOD, the key acquisitions underway to build the GIG network capability include 1) Transformational Satellite[3] (TSAT), a new constellation of communications satellites to transmit and route larger volumes of data; 2) Joint Tactical Radio System (JTRS), a new family of interoperable radio systems; 3) Global Information Grid-Bandwidth Expansion (GIG-BE), which includes state of the art optical network technologies and upgraded routers and switches to increase bandwidth for greater voice, data, and video transmissions as well as improvements in

[3] TSAT is one of six initiatives under development as part of the Transformational Communications System Initiative.

network services at about 90 DOD installations; 4) Network Centric Enterprise Services (NCES), a common set of services and applications to manage the network and help users locate and share information; 5) Cryptography Transformation Initiative,[4] tools to protect sensitive information transmitted across the network and protect the network from attack; and 6) Horizontal Fusion, which is a portfolio of initiatives focused on developing and demonstrating data applications and tools for information sharing and netcentric operations.

Table 3 reviews each of the key acquisitions for the GIG's core capability, including the purpose, the financial investment between fiscal years 2004 and 2009, the military service or defense agency responsible for managing the acquisition, and the current status. Some of these acquisitions will require funding, including sustainment costs, beyond 2009 but amounts are not yet known.

[4] The Cryptography Transformation Initiative is part of DOD's broader Information Assurance program, which includes many security initiatives critical to the GIG. The cryptography initiative is funded from different program elements within DOD's Information Assurance program.

Table 3: Overview of Six Major Acquisitions Related to the Core GIG Network and Information Capability

Program or initiative	Purpose	Investment (fiscal years 2004 to 2009)	Manager	Status
TSAT	To develop satellites to serve as the cornerstone of a new DOD communications infrastructure and provide high bandwidth connectivity to the warfighter. Some of the technologies that TSAT plans to use are laser cross-links, space-based data processing and Internet routing systems, and highly agile multibeam/phased array antennas.	$8.5 billion	Air Force.	Product development began in early fiscal year 2004; first satellite scheduled to launch in 2011.
JTRS	To develop family of software-defined radios to interoperate with different types of existing radios and significantly increase voice, data, and video communications capabilities.	$5.8 billion	Joint service program responsible for the software communications architecture and waveforms; military service-led programs responsible for developing radios.	Army is leading the development of a cluster of radios for ground vehicles and helicopters. This cluster began in 2002; the first radios are to be fielded in fiscal year 2007.
GIG-BE	To provide additional bandwidth and information access at key military installations within the United States and overseas via a combination of acquiring bandwidth from commercial providers as well as extending fiber optic networks to bases and installations that are located away from commercial networks.	$373 million	Defense Information Systems Agency.	Procurement phase began in 2003. Initially, 10 sites to be completed this year and the remaining sites in 2005.

Program or initiative	Purpose	Investment (fiscal years 2004 to 2009)	Manager	Status
NCES	To enable network users to identify, access, send, store, and protect information. Also to enable DOD to monitor and manage network performance and problems. Is expected to require development of new capabilities and tools for tagging data so it is useful, providing users with capability to identify relevant information based on content and allowing users to freely exchange and collaborate on information.	$371 million	Defense Information Systems Agency.	In concept phase; product development to begin in fiscal year 2004; initial set of core services to be provided beginning in fiscal year 2005.
Crypto Transformation Initiative	To enable DOD to protect the network and sensitive information. To provide information assurance and encryption support, including cryptography equipment (e.g., Internet protocol encryptors), firewalls, intrusion detection systems, etc.	$4.8 billion	National Security Agency, Defense Information Systems Agency, and the military services.	The National Security Agency is developing information assurance component of GIG architecture; other ongoing efforts to develop enhanced encryption capabilities.
Horizontal Fusion	A portfolio of initiatives, drawn from existing programs, intended to demonstrate netcentric capabilities and address operational and technical challenges. Initiative underway, for example, to Web-enable current data sources, tools, and applications.	$1.3 billion	Office of the Secretary of Defense for Networks and Information Integration.	Ongoing program. Initial set of initiatives funded in fiscal year 2003. Annual demonstrations known as "Quantum Leap" conducted on initiatives.

Sources: DOD (data); GAO (analysis).

In developing the GIG's core capability, DOD intends to build upon and enhance ongoing terrestrial and space-based networks and systems, such as the Advanced Extremely High Frequency satellite communication system and the Defense Information Systems Network. The new programs underway are intended to improve communications and networking capabilities significantly. For example, according to DOD officials, current telecommunication lines are not robust enough to handle the volume of information needed to facilitate optimal, strategic decision making. The GIG-BE is designed to remove current bandwidth constraints. The GIG-BE is to use advanced fiber-optic backbone and switching technology to upgrade telecommunications lines and provide initially up to 10 gigabytes

per second of bandwidth at selected defense installations around the world. Also, unlike DOD's legacy radio systems that cannot interoperate with one another, JTRS is software-based, meaning that the radios are essentially computers that can be programmed to imitate other types of radios and thus be readily configured to operate in different networks and waveforms[5] based on common standards. JTRS is expected to act as a gateway for users with different hardware radios—a capability that speeds the transition to universal interoperability for DOD military operations. Also, unlike current communication satellites, TSAT is to be equipped with laser-optical payloads for high-capacity links to other air and space platforms. By using laser-optics, TSAT is intended to operate above the radiofrequency spectrum and provide relief to current military bandwidth constraints. NCES is to make use of commercial products and tools to manage messaging, storage, search, and other capabilities across platforms, but also require new and possibly customized services to ensure the sharing of information based on mission demands and priorities. Tools to allow users to "smartly" pull and fuse information will require investing in new data content and management techniques. Enhanced security (information assurance)[6] capabilities will need to be developed, including encryption mechanisms and devices, intrusion detection systems, and secure network management.

Other Acquisitions That Must Be Integrated with the GIG Core Network

Most ongoing and planned weapon systems; command, control and communications systems; and business systems will need to be integrated with the GIG network, because they will be the primary providers and receivers of data needed to support future military operations.

- DOD plans to integrate most weapon systems into the GIG. In fact, some "transformational" weapon systems now under development require a more advanced communications infrastructure to perform as

[5] A waveform is the representation of a signal that includes the frequency, modulation type, message format, and/or transmission system. In general usage, the term waveform refers to a known set of characteristics, for example, frequency bands (VHF, HF, UHF), modulation techniques (FM, AM), message standards, and transmission systems. In JTRS, the term waveform is used to describe the entire set of radio functions that occur from the user input to the radiofrequency output and vice versa.

[6] "Information assurance is defined by DOD as measures that protect and defend information and 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. "Department of Defense Directive 8500.1, *Information Assurance*, October 24, 2002 (Certified current as of Nov. 21, 2003), Section E2.1.17.

intended and to support voice, data, videoconferencing, and imagery transmissions. Without an integrated network that ties together different systems and enables information to flow freely across the battlefield, the high-paced warfare that DOD envisioned is likely to be constrained, according to DOD. For example, the Army is developing the Future Combat Systems, a new generation of manned and unmanned ground vehicles, air vehicles, and munitions that are to be lighter and more mobile yet lethal and survivable. Rather than rely on heavy armor to withstand an enemy attack, the Future Combat Systems will depend on superior information to see and kill the enemy before being detected. According to DOD, the ability to make this leap depends on (1) a network to collect, process, and deliver vast amounts of information, such as imagery and data, and (2) the performance of the individual systems themselves. Not only must systems within the Future Combat Systems interoperate effectively, they also must interoperate with the GIG. The GIG must perform at a level that enables the Future Combat Systems to quickly collect, process, and deliver data. DOD is also developing a new constellation of satellites—known as Space-Based Radar—to provide a near continuous, all-weather global capability of collecting intelligence, surveillance, and reconnaissance[7] information. Space-Based Radar is expected to be a critical data provider to transformational systems, such as those within the Future Combat Systems. Like the Future Combat Systems, the satellites will require a more robust communications infrastructure to send massive amounts of imagery data in a timely fashion. According to DOD, if TSAT, a key GIG component, is not ready in time or cannot provide the capability originally planned, DOD may need to build additional capability into Space-Based Radar satellites and ground stations to reduce the dependency on the communications infrastructure to transmit data.[8]

- DOD intends to integrate virtually all command, control, and communications, systems into the GIG. At the same time, DOD intends to develop and modify these systems to provide military commanders

[7] Intelligence is defined by DOD as the product resulting from the collection, processing, integration, analysis, and evaluation of information. Surveillance is the systematic observation of places, persons, or things through visual and other means. Reconnaissance is a mission undertaken to obtain information about activities and resources of an enemy or potential enemy or to secure data characteristics of a particular area.

[8] U.S. General Accounting Office, *Defense Acquisitions: Space-Based Radar Effort Needs Additional Knowledge Before Starting Development*, GAO-04-759 (Washington, D.C.: July 23, 2004).

and forces with near-real time descriptions of the location and disposition of U.S. military forces and adversaries operating on the ground and in the air and to provide the ability to communicate across all elements involved in military operations. Each of the military services has major architectural initiatives underway (the Air Force's C2 Constellation and ConstellationNet, the Army's LandWarNet, and the Navy's ForceNet) to transform their command, control, and communications systems and information infrastructures into the GIG. For example, the Army's Warfighter Information Network-Tactical (WIN-T) program (part of LandWarNet) is intended to be the integrating communications network that links Future Combat Systems units with higher Army echelons and with the GIG. In addition, DOD considers numerous other systems to be important in achieving the GIG, including the Mobile User Objective System (satellite communications), Global Command and Control System/Joint Command and Control, Deployed Joint Command and Control, and Teleports (information transport system). DOD has further identified the need to eventually link the GIG to coalition, allied, and non-DOD users and systems.

- DOD also intends to integrate its business systems into the GIG. These include acquisition and procurement systems, financial management systems, personnel and health systems, logistics systems, and strategic planning and budgeting systems. Many of these play an important role in supporting military operations. For example, logistics systems are used to plan, control, and carry out the efficient and effective movement and maintenance of forces.

Implementation

The GIG's success is dependent on DOD's ability to successfully integrate the majority of its weapon systems, command, control, and communications systems, and business systems with the new core network. To make this happen, DOD has developed a blueprint or architecture for the GIG; developed new policies, guidance, and standards to guide implementation decisions; undertaken proactive efforts to "market" the GIG and its potential benefits; and is attempting to influence key budgeting and acquisition decision-making processes to align with the GIG concept.

Architecture and Policies

To help guide decision-making, DOD has developed an initial architecture for the GIG, which, according to DOD, presents the current information technology environment and desired (target) technology environment; describes how the commands, services, and defense agencies will operate in a netcentric environment, based on selected strategic, operational, and

tactical scenarios; and identifies the actions and information requirements for conducting operations in a netcentric environment, how systems will need to function to access information, and emerging standards for the development and acquisition of systems. DOD also has developed a reference model so program managers of various architectures and systems can ensure GIG compliance.[9] According to DOD, the reference model's key purpose is to provide users with an understanding of the GIG through common definitions and terms of reference, standards, and templates for developing more detailed architectures. Future versions of the GIG architecture are to include more complete views of DOD's operational environment and existing enterprise requirements. Furthermore, DOD is modifying its Joint Technical Architecture,[10] which sets standard technologies and protocols to better ensure interoperability and to complement the GIG architecture.

DOD is also in the process of issuing new policies, standards, and guidance to formalize the architecture. Specifically, DOD has created policy that requires all departmental architectures to be GIG compliant. DOD also has developed specific policies, standards, and guidance to implement the GIG and help ensure that the military services acquire systems that integrate with the GIG. Several policies establish the GIG as a cornerstone for enabling DOD to achieve information superiority, formally define the objectives and key elements of the GIG, and assign roles and responsibilities for the GIG on an enterprise basis. Others assign responsibility and define waiver procedures for specific aspects of the GIG, such as ground-based telecommunications networks and NCES. For example, DOD formalized a waiver process to assess network and telecommunications systems (such as local area networks) that are not GIG-compliant. In addition, DOD has set standards to address data connectivity. To provide a common format for the transmission of information across the GIG, DOD recently mandated that GIG systems

[9] Referred to as the *Netcentric Operations Warfare Reference Model*, Version 1.0, December 2003.

[10] For several years, DOD has emphasized the use of a framework that defines three types of architectures: operational, technical, and system. A technical architecture is a set of rules to guide the design of systems and consists primarily of a common set of standards and protocols for sending and receiving information (e.g., Internet protocol), understanding information (e.g., format standards), and processing the information. The Joint Technical Architecture specifies the minimum set of standards and guidance for the acquisition of all DOD systems that produce, use, or exchange information.

must be Internet Protocol Version 6[11] capable, as well as Internet Protocol Version 4 (the Internet currently is based on version 4.),[12] or obtain a waiver. Furthermore, DOD developed a netcentric data strategy, standardizing the way data will be described and used in systems that make up the GIG. Appendix I provides more details on these policies, standards, and guidance.

Influencing Acquisition and Budgeting Decisions

DOD officials who developed the GIG concept also expect to influence decisions by participating in DOD's key decision-making processes. Over the past couple years, DOD has revised its three primary decision-making processes for determining and delivering military capabilities—requirements setting, acquisition, and budgeting—to focus acquisitions and investment decisions on meeting joint mission needs, particularly with regard to interoperability. In revising these processes, DOD has emphasized compliance with the GIG architecture. DOD officials have taken further action intended to strengthen these decisions by developing tools and criteria for actively participating in the decision-making process—by assisting military services in preparing for major acquisition reviews (as part of integrated product teams) and/or by providing input to decision-making boards. The revisions DOD has made to its requirements setting, acquisition, and budgeting process are all fairly recent. Therefore, it is too early to assess whether they will be successful in achieving their goals.

For example, DOD revised its requirements-setting process to shift the focus to a more capabilities-based approach for determining joint war-fighting needs rather than a threat-based approach focused on individual systems and platforms. Under the threat-based approach, the services were primarily responsible for defining requirements, selecting alternatives, and developing systems, which frequently resulted in the fielding of stovepiped systems and duplicating capabilities. DOD's rationale for shifting to capabilities-based requirements is a recognition

[11] Internet protocol specifies the format of packets, also called "datagrams," and the addressing scheme for communication transmissions and virtual connections made over the Internet. Internet Protocol Version 6 (also referred to as IPv6) is the latest version of this protocol.

[12] IPv6 includes a transition mechanism that is designed to allow users to adopt and deploy IPv6 in a highly diffuse fashion and to provide direct interoperability between IPv4 and IPv6 hosts. The transition to a new version of the Internet Protocol is intended to be incremental and allow users to upgrade their hosts to IPv6, and network operators to deploy IPv6 in routers, with very little coordination between the two.

that there is greater uncertainty in future military conflicts without a clearly defined adversary and it will need to respond across a broader range of military operations. The new Joint Capabilities Integration and Development System, established in October 2003, is organized around key functional concepts and areas—command and control, force application, battlespace awareness, focused logistics, and force protection–aimed at improving joint warfighting capabilities. In addition, a sixth area has been established—netcentric operations—to enable planning across functional areas and support integration of netcentric capabilities. The Office of the Assistant Secretary of Defense for Networks and Information Integration and Joint Staff officials believe the joint concept will provide a more coherent framework for identifying capabilities gaps, comparing alternatives, aligning requirements to the GIG, and reduce the potential for stovepiped, duplicative capabilities.

DOD officials also indicated that the department has begun revising its planning and budgeting process in an effort to instill more collaboration among different components of the department in investment decisions. For example, DOD is asking the military services to plan budgets around guidance that takes a joint perspective. Data collection and management processes are intended to be merged into a portfolio management approach that enables program reviews and budget reviews to occur in a more integrated manner rather than sequentially. To complement this process, DOD is planning to develop an investment portfolio management structure to better manage its information technology resources where decisions about what information technology investments to make, modify, or terminate, are based on the GIG architecture and other objectives, such as mission area goals. Other recent policies have focused on establishing more effective investment processes for information technology systems that need to integrate with the GIG.

DOD has developed several mechanisms to complement the decision making that occurs within the Joint Capabilities Integration and Development System, planning and budgeting, and acquisition processes. For example, in November 2003, the Office of the Assistant Secretary of Defense for Networks and Information Integration, in consultation with the Joint Chiefs of Staff, Office of the Under Secretary of Defense for Acquisition Technology and Logistics, and U.S. Joint Forces Command,

established a new Net-Ready Key Performance Parameter[13] and review process to focus greater attention on systems interoperability for joint operations as well as the information-sharing requirements of the GIG. The Net-Ready Key Performance Parameter is built around compliance with the GIG architecture, and the reference model will be used to assess system information needs, information assurance, and the technical exchange of information. The Office of the Assistant Secretary of Defense for Networks and Information Integration has also developed a netcentric checklist to guide the Joint Capabilities Integration and Development System and acquisition reviews. The checklist is based on the GIG architecture and will be used to assess whether key standards and protocols are being considered and built into particular capabilities and systems being acquired. In addition, the Office of the Assistant Secretary of Defense for Network and Information Integration has established a systems engineering and evaluation capability to support the reviews. A team of systems engineers will provide end-to-end technical support to the office and funding has been requested to create a facility to test key GIG-related systems and components. DOD will be conducting specific netcentric reviews of major acquisition programs to assess whether they are transitioning to integrate with the future network. About 129 information technology, weapon systems, and business systems have been selected to participate in the initial round of assessments. These reviews are scheduled to be completed later this year.

DOD Challenges in Implementing the GIG

The most critical challenge ahead for DOD is making the GIG a reality. While DOD has taken steps to define its vision and objectives for the GIG on paper and in policy, it is not fully known how DOD will meet these objectives, particularly with respect to setting investment priorities, providing management attention and oversight, transforming operations, and advancing technologies. At the same time, DOD is beginning to make a heavy investment in the GIG as well as systems that will be heavily dependent on the GIG, such as the Army's Future Combat Systems, and DOD is asking its components and the military services to accept its vision and plan toward it. In addition, DOD faces risks inherent with the nature and scope of the effort it is undertaking, for example, risks related to protecting data within the thousands of systems that will be integrated

[13] A key performance parameter represent those critical performance parameters so significant that a failure to meet a minimum value of performance can call into question a system's ability to perform missions.

into the network. DOD recognizes these challenges, and many of the actions it is taking to implement the GIG are meant to address them. However, it is too early to assess how successful DOD will be in addressing the challenges and overcoming long-standing organizational impediments.

Table 4 below highlights some of the key challenges facing DOD.

Table 4: Key Challenges

Management and investment	• Deciding what capabilities are affordable; what capabilities are unaffordable or not in line with DOD's vision for the GIG, and enforcing these decisions among thousands of systems and across the military services. Assuring DOD has the right representation in acquisition decisions. • Assuring management attention and oversight is provided to assess the overall progress of the GIG and determine whether it is providing a worthwhile return on investment, particularly in terms of enhancing and even transforming military operations.
Operational	• Deciding when, how, and how much information should be posted on the network and used. • Establishing rules to ensure the GIG can work as intended without reducing benefits of flexible and dynamic information sharing. • Convincing data owners of the value of sharing data with a broader audience and trusting the network enough to post data.
Technical	• Developing new technologies and advancing them on schedule. • Assuring common agreement on technical as well as information assurance standards and requirements. • Developing the means to protect the network and its data.

Source: GAO analysis.

Management and Investment Challenges

While DOD has taken steps to establish a vision and objectives for the GIG, it is still not fully known how DOD will manage, oversee, and invest in this effort. Addressing these questions is a daunting task. DOD must find ways to make and enforce trade-off decisions for literally thousands of information technology systems, weapon systems, command and control

systems, intelligence systems, and other systems.[14] These decisions will need to span a wide range of organizations, including the military services and their respective major commands and functional activities, numerous large defense agencies and field activities, and various combatant and joint operational commands that are responsible for military operations for specific geographic regions or theaters of operations. Having accurate and reliable visibility over spending on systems that must integrate with the GIG will be necessary as well as having effective mechanisms for identifying and deciding which systems should be pursued and which should not. In 2003, we reported (as part of a survey of federal agencies enterprise architecture programs) that DOD had made progress in developing the GIG architecture, however, the department had not completed some essential architecture products that describe the desired (target) technology environment and provide a sequencing plan for transitioning to it.[15] More specifically, at this point, DOD is largely leaving it up to its components and services to decide how best to migrate their systems to the GIG. There is no well-defined strategy that

- identifies what capabilities DOD will invest in and what it will not invest in;
- identifies how investments will align with the goals and objectives of the GIG architecture;
- determines what is affordable, particularly in light of near-term and long-term needs;
- sets out criteria for determining what legacy systems should remain or be phased out; and
- specifies by whom and how decisions will be enforced.

In addition, it is unknown how senior leaders within DOD will be able to focus on the progress of the GIG as a whole, that is, whether it is being developed and fielded within cost and schedule, whether risks are being adequately mitigated, and whether the GIG is providing a worthwhile return on investment, particularly in terms of enhancing military operations. Until DOD implements an investment and oversight strategy

[14] DOD's information technology budget (covering national security and business systems) for fiscal year 2004 totaled about $28 billion. Of this, about $10.5 billion was for modernizing systems and the remaining $17.5 billion for operating and maintaining existing systems.

[15] U. S. General Accounting Office, *Information Technology: Leadership Remains Key to Agencies Making Progress on Enterprise Architecture Efforts*, GAO-04-40 (Washington, D.C.: Nov. 17, 2003).

for the GIG as a whole, it is at risk of making investments that do not fit its vision for the future.

According to DOD officials, the enhancements DOD is making to its planning and budgeting processes are meant to begin addressing these questions. However, these changes may be difficult to implement for a number of reasons. First, to some degree because of the broad scope and crosscutting nature of the GIG concept, no office or single program is in charge of the GIG, making it more difficult to make and enforce trade-off decisions. Moreover, while key acquisition, budgeting, and requirements setting processes have been modified, they still largely operate under the same organizational structure, where it has been difficult to link acquisition and investment decisions to joint concepts like the GIG.

Additionally, previous efforts that have been undertaken in past years to foster interoperability among DOD systems have had limited success, principally because management tools and leadership attention were not strong enough to provide sufficient oversight and overcome resistance by the military services to forgo their unique requirements in favor of requirements that would benefit the department, as the following examples illustrate:

- In our 2001 report[16] on DOD's efforts to improve its ability to attack time-critical targets, we noted that DOD had undertaken numerous efforts to achieve system interoperability, including the development of guidance, oversight controls, directives and policies, and technology demonstrations. However, success was limited because DOD had not yet overcome resistance from the military services, it lacked an architecture to guide interoperability efforts and some current oversight and control mechanisms, such as the interoperability certification process, were not working or were not being enforced.

- In 2003, we reported[17] that two joint acquisition programs lacked mechanisms to overcome parochialism and stovepipes at the military service level. The JTRS program lacked a strong management structure

[16] U.S. General Accounting Office, *Joint Warfighting: Attacking Time-Critical Targets*, GAO-02-204R (Washington, D.C.: Nov. 30, 2001).

[17]U.S. General Accounting Office, *Challenges and Risks Associated with the Joint Tactical Radio System Program*, GAO-03-879R (Washington, D.C.: Aug. 11, 2003) and *Force Structure: Improved Strategic Planning Can Enhance DOD's Unmanned Aerial Vehicles Efforts*, GAO-04-342 (Washington, D.C.: Mar. 17, 2004).

to resolve operational requirements and funding issues among the services and DOD's approach to planning Unmanned Aerial Vehicles lacked an effective strategic plan to ensure the military services and other defense agencies focus their development efforts on systems that complement each other.

- In 2004, we reported[18] that DOD was making limited progress with its business modernization initiative—a departmentwide effort focused on transforming DOD business operations, including standardizing and optimizing business systems across DOD and reducing duplication. After 3 years of effort, we reported that we have not seen any significant change in the content of DOD's business systems modernization architecture (which is to be integrated into the GIG architecture) or in DOD's approach to investing billions of dollars in existing and new business systems. Further, DOD had not yet implemented an effective management structure and processes to provide adequate control and accountability over its $5 billion annual investment in business systems modernization. In particular, we reported that DOD had not yet clearly defined the roles and responsibilities for its new business investment domains, established common investment criteria, and conducted a comprehensive review of its existing business systems to ensure that they are consistent with the business modernization architecture. DOD acknowledged that it still had much more to do, including developing the business systems modernization architecture to a necessary level of detail, defining specific performance metrics, and clarifying the roles and responsibilities associated with managing the domains of portfolios of business systems and ensuring that these systems comply with the architecture.

Several recent studies sponsored by DOD recognize that developing an investment strategy and adopting better management tools is critical for the success of the GIG. For example, a 1999 Defense Science Board study[19] assessed DOD's strategies and processes for attaining information

[18] U.S. General Accounting Office, *DOD Business Systems Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments*, GAO-04-731R (Washington, D.C.: May 17, 2004) and *Department of Defense: Further Actions Needed to Establish and Implement a Framework for Successful Financial and Business Management Transformation*, GAO-04-551T (Washington, D.C.: Mar. 23, 2004).

[19] Defense Science Board Task Force, *Tactical Battlefield Communications* (Washington, D.C.: Dec. 1999).

superiority and advocated that (1) an executive office be established to lead and implement the GIG and that (2) the office develop an implementation plan, including technical milestones and measurable interim goals, and identify resources to permit the transition to and completion of the GIG. A 2004 report by the U.S. Joint Forces Command,[20] documenting the processes and planned activities underway to achieve transformational improvements in joint military capabilities, recommended, among other things, that the GIG should include a time-phased plan for how future capabilities will link to current investments. In addition, the report recommends that such a plan should show how network development efforts underway by each of the military services will contribute to and be compatible with the GIG.

Other studies have pointed to the need to strengthen current management processes to ensure warfighters themselves have more input into investment decisions. For example, a 2003 study[21] chartered by the Secretary of Defense to examine how DOD develops, resources and provides joint capabilities, recommended moderate to more radical actions to streamline existing processes and/or establish alternative organizations to better integrate defense capabilities in support of joint military objectives. Organizational alternatives for strengthening the acquisition process ranged from the establishment of joint program executives for each of the Joint Capabilities Integration and Development System's functional capabilities areas that would provide input and oversee resources on joint programs, to capability acquisition executives for each of the capability areas who would have direct oversight and decision authority over all programs. A 2004 study by the Center for Strategic and International Studies[22] identified defense reforms needed to meet the challenges of a new strategic era and made a number of recommendations, including several to improve the acquisition of joint capabilities and establish a more effective resource allocation process. For example, the study recommended that the Joint Staff (J-6—Command, Control, Communications, and Computers) be expanded into a

[20] U.S. Joint Forces Command, *Joint Transformation Roadmap* (Washington, D.C.: Jan. 21, 2004).

[21] Joint Defense Capabilities Study Team, *Joint Defense Capabilities Study: Final Report* (Washington, D.C.: Dec. 2003).

[22] C.A. Murdock et al, *Beyond Goldwater-Nichols: Defense Reform for a New Strategic Era*, *Phase 1 Report* (Washington, D.C.: Center for Strategic and International Studies, Mar. 2004).

departmentwide, joint task force with budgetary and acquisition authority for joint command and control capabilities. In addition, to improve trade-off decisions across mission areas, the study advocates building capacities in the combatant commands for a stronger role in the resource allocation process.

Operational Challenges

There are also many unknowns concerning how DOD will meet its requirements and vision in terms of people, processes, and, ultimately, operations. First, DOD has yet to determine how much information should be posted on the network; when it should be posted; and how and where it should be used. Once these factors are determined, DOD must develop rules of operation to ensure the network can work as intended without precluding the benefits that can be derived from more flexible and dynamic information sharing. Currently, various offices within DOD are working through questions on whether unlimited amounts of data should be made available through the GIG, including unprocessed intelligence, surveillance, and reconnaissance data, without the benefit of some assimilation and analysis. These are important questions that need to be addressed in the near future because they could affect the direction of investments in netcentric systems and non-network systems as well as changes that need to be made in how the intelligence community operates.

Even after these questions are settled, significant operational challenges remain. Joint commanders and the military services may need to find ways to adapt to an environment where data can be more readily obtained and shared by lower levels in the chains of command. New operational concepts are being developed to guide how military operations are to be conducted in this enhanced technology environment. They will need to be followed by associated doctrine, tactics, techniques, and procedures. Developing joint operational concepts is one of the key tenets under the Joint Capabilities Integration and Development System; however, it is unclear how the concepts will be developed and translated by these boards into more detailed tactics, techniques and procedures. We recently reported that DOD had been proceeding with the JTRS program for several years without clear definition of how JTRS capabilities should be used in an operational environment and that the program's concept of operations did not reflect the joint vision of JTRS but instead the service-centric radio-replacement perspective. If DOD is to achieve its long-term goals for netcentric warfare, it is imperative that it develop concepts and processes for how individual systems, such as JTRS, can be used to leverage DOD's new network infrastructure and maximize interoperability and collaboration in military operations.

Moreover, DOD must successfully persuade data owners to accept the value of sharing data with a broader audience and to trust the network enough to post data. We spoke with several officials in charge of GIG programs who acknowledged that facilitating these cultural changes—particularly with the intelligence community—will be difficult.

In addition, DOD also faces a formidable task in persuading the military services and other users of the network to rely on information technology applications and services being developed by the Defense Information Systems Agency. This agency has been tasked with developing and providing key voice, video, and data connectivity through core enterprise services for the GIG, such as data query (search or discovery) capabilities and information assurance. However, the military services and defense agencies have historically been reluctant to rely on the Defense Information Systems Agency for these services. We have reported in the past that the military services have regularly bypassed Defense Information Systems Agency, preferring instead to procure their own telecommunications networks and commercial satellites bandwidth services because they were dissatisfied with the level of service provided by the agency as well as the cost and length of time it took to procure these services centrally.[23]

Technical Challenges

Building a reliable, secure network that will operate on the move, virtually anywhere and provide the necessary information and services to enable netcentric military operations presents considerable technical challenges. While DOD intends to utilize existing commercial communications and networking technologies, which have advanced significantly in recent years, the GIG requires DOD to advance a number of key technologies, develop a series of complex systems and software, field them without delay so schedules for other dependent systems are not disrupted, and develop the means to effectively manage and protect the network and its data.

[23] U.S. General Accounting Office, *Satellite Communications: Strategic Approach for DOD's Procurement of Commercial Satellite Bandwidth*, GAO-04-206 (Washington, D.C.: Dec. 10, 2003); *Defense Networks: Management Information Shortfalls Hinder Defense Efforts to Meet DISN Goals*, GAO/AIMD-98-202 (Washington, D.C.: July 30, 1998); and *Defense IRM: Investments at Risk for DOD Computer Centers*, GAO/AIMD-97-39 (Washington, D.C.: Apr. 4, 1997).

At this time, however, DOD is pushing ahead on several programs with immature technologies and with aggressive development and fielding schedules. As a result, DOD is at risk of not delivering required capabilities within budgeted resources. This, in turn, may affect schedules and funding for other systems depending on the GIG. For example, two key GIG-related programs—JTRS and TSAT—are facing schedule and performance risks, which are largely rooted in attempts to move these programs into product development without sufficient knowledge that their technologies can work as intended. In March 2004, we reported that none of the 20 critical hardware and software technologies for the Army's initial JTRS radio development for ground vehicles and helicopters were sufficiently mature according to best practice standards.[24] When product development began in June 2002, the Army determined that while many of the technologies within the program had been used in other radio applications, they could not be assessed as mature because they had not been integrated into a complex radio, such as JTRS. Mature backup technologies exist for some critical technologies, but program officials have cautioned that substituting them could complicate integration or result in degraded performance. Moreover, the program recently experienced a 4-month schedule slip that officials attribute to short-term technology deviations affecting size, weight, and power requirements for the radio sets. Further, the program entered product development with an ambitious schedule that program officials recognized as high risk. In particular, the program has a compressed test and evaluation phase that leaves little room for error and rework.

We also recently reported that the TSAT program entered into product development with only one of its six critical technologies sufficiently mature. The remaining five technologies are not expected to reach maturity until 2006. Backup technologies exist for three of the five immature technologies, but they would degrade system performance. The other technology—single access laser communications—has no backup and program officials indicated any delay in maturing this technology

[24] GAO has conducted a body of work on best practices and found that programs managed within a knowledge-based approach—where levels of product knowledge are demonstrated at critical points during development—are better positioned to deliver superior performance within cost and schedule estimates. For example, a match between program requirements and resources (mature technology, time, and funding) at the start of product development is particularly important. A high level of technology, time, and funding) at the start of product development is particularly important. A high level of technology maturity means that the technologies needed to meet essential product requirements have been demonstrated in their intended environment.

would cause the first satellite launch date to slip significantly. DOD believes it has adequate measures to mitigate these risks, however, concern over TSAT technology readiness led the Air Force to schedule an interim review for November 2004, which will determine whether the program's technology development has progressed sufficiently or whether alternative action should be taken.

Similar risks extend to the systems that must be integrated with the GIG and on which DOD is dependent for achieving its vision for netcentric warfare. For example, our review of the Future Combat Systems determined that the program is at significant risk, in part because more than 75 percent of its critical technologies were immature at the start of development and many will not be sufficiently mature until the production decision.[25] First prototypes for the systems that make up the Future Combat Systems will not be delivered until just before the production decision, and full demonstration of the Future Combat Systems' ability to work and meet its goals will not occur until after production has begun. If the lessons learned from best practices and the experiences of past programs have any bearing, the Future Combat Systems program is likely to encounter "late-cycle churn," a phrase used by private industry to describe the discovery of significant problems late in development and the resulting search for fixes when costs are high and time is short.

Networking, network management, and secure network management challenges are considerable.[26] Currently, mobile networking is limited, mainly to narrowband, fixed infrastructures, and relatively stable user groups. The GIG network will require new wideband waveforms that can handle the expected high data rates, throughput of information, and ability to transmit integrated voice, data, and video simultaneously. In addition, dynamic networking capabilities that can automatically adjust to changing circumstances, such as intrusions or node failures, are needed; however,

[25] U.S. General Accounting Office, *Defense Acquisitions: The Army's Future Combat Systems' Features, Risks, and Alternatives*, GAO-04-635T (Washington, D.C.: Apr. 1, 2004).

[26] GAO has defined five categories of cybersecurity controls: (1) access control; (2) system integrity; (3) cryptography; (4) audit and monitoring; and (5) configuration management and assurance, that can help as safeguards and countermeasures to protect agencies' information technology networks such as the GIG network. Agencies such as DOD can use network management to control and monitor networks to obtain status data from components, make configuration changes, and alert network managers to problems. See U.S. General Accounting Office, *Information Security: Technologies to Secure Federal Systems*, GAO-04-467 (Washington, D.C.: Mar. 9, 2004).

the scalability of network management technologies for a network like the GIG with such a large number of nodes is unproven. To facilitate timely and prioritized access to information from a wide variety of sources, the network will require enhanced quality of service mechanisms and algorithms to manage bandwidth allocation and handle the flow of information and security. Furthermore, advances will be needed in several other technological areas, such as antennas, power sources, and the miniaturization of components to facilitate mobile communications. For example, current antennas do not support all of the portions of the radio frequency spectrum where the GIG network will operate and are limited to specific communications waveforms. Advanced multiband antennas will be needed to support mobile and simultaneous communications across different portions of the spectrum.

Integrating other elements of the network will also be challenging. The increased bandwidth capability provided by the GIG-BE program may not be fully realized if the military services and defense agencies do not use compatible technologies and protocols in upgrading their networks. Even if the technologies and protocols are compatible, bandwidth may be limited if these networks are not properly designed and integrated to manage voice, data, and imagery transmissions. Network management policies may pose challenges if common agreement cannot be reached across the military services and defense agencies on standards and information assurance requirements. For example, DOD and the intelligence community have not yet reached agreement on how they will exchange information and verify security credentials on the GIG network.

Information assurance itself may be one of the most critical challenges facing DOD. While building a network based on Internet protocols is expected by DOD to provide a more viable path to achieve interoperability and enable more dynamic and flexible information sharing, it also exposes DOD to the same vulnerabilities that face all users of the Internet, and it increases the opportunity for potential attackers with limited knowledge and technical skills to cause a great deal of damage. Establishing network and system security safeguards—such as firewalls, identifying the sender and recipient of information, protecting information from unauthorized access, and safeguarding data to prevent accidental and deliberate alterations—will be essential but difficult given the size the network and the thousands of systems and users that will be linked to it.

Moreover, if the network is to be used to provide warfighters on the move with access to intelligence and other sensitive information on demand, information will need to be encrypted to safeguard data from misuse.[27] However, the technologies needed to secure communications, such as software programmable encryption devices are still in their infancy. Further, the complexity and magnitude of enabling hundreds of systems and applications to operate in a secure, Web-based environment will require careful planning and coordination. Comprehensive plans will be needed to ensure that sensitive data and communications are safeguarded across diverse platforms. This will require DOD to identify sensitive data as well as applications, databases, storage subsystems, and media used to process and store the data. Once systems have been examined, data access models must be applied to determine proper security levels for information and how integration can occur across platforms without disrupting network and near-real time operations. No one security solution likely will address GIG requirements.

Lastly, the enterprise information services planned for the GIG pose timing challenges. For example, in the near-term, DOD has established a goal to complete the transition to Internet Protocol Version 6 by fiscal year 2008. According DOD officials, the commercial industry may not be able to provide the necessary products for Internet Protocol Version 6 by the targeted milestone. Also, the transition will not be completed until a Joint Staff developed set of performance and technical criteria can be met. In addition, because of the enormous amount of data that will become available, new data fusion methods will need to be developed to help users rapidly identify, access, and make sense of available information.

Conclusions

DOD is depending on the GIG to enable a fundamental transformation in the way military operations are conducted. While DOD's vision of the GIG is compelling, the breadth and depth of the GIG and DOD's objectives for netcentric warfare, present enormous challenges and risks—many of which have not been successfully overcome in smaller-scale efforts and many of which require significant changes in DOD's culture. Moreover, even though DOD has begun to make heavy investments to implement the new network and to ask the military services to accept its vision for the GIG, important questions as to how DOD will make the GIG a reality and

[27] Cryptographic transformation involves altering data into a form that conceals that data's original meaning to prevent it from being known or used.

how it will oversee progress as a whole and ensure the GIG is providing an adequate return on DOD's investment are only just beginning to be addressed, leaving DOD at risk of making investments that may not fit in with its vision for the future. Moreover, many new weapon systems and sensors, which are costing DOD tens of billions of dollars, are critically dependent on the future network to successfully achieve their own capabilities. Any disruptions in the schedule for key systems that support the network, therefore, can have significant ramifications. As such, it is important that DOD ensure it has sufficient knowledge about these systems (e.g., requirements, technologies, security) as it makes additional commitments to them and that it has effective risk mitigation plans to ensure that they can deliver promised capability on time. Our future work, therefore, will assess DOD's progress in addressing these challenges in more depth as well as its progress in managing key acquisitions related to the GIG.

Agency Comments

DOD provided technical comments on a draft of this report that we incorporated where appropriate.

We plan to provide copies of this report to the Secretary of Defense, the Assistant Secretary of Defense for Networks and Information Integration, the Under Secretary of Defense for Acquisition, Technology and Logistics, the Under Secretary of Defense (Comptroller), the Director of the Defense Information Systems Agency, and interested congressional committees. We will make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-3519, Cristina Chaplain at (202) 512-4859, or John Oppenheim at (202) 512-3111. Other individuals making key contributions to this report are Lily Chin, Arturo Holguin, and Yvonne Vigil.

Robert E. Levin
Director
Acquisition and Sourcing Management

Appendix I: Policies, Standards, and Guidance to Implement the Global Information Grid

Table 5: Selected Global Information Grid Policies, Standards, and Guidance (2000 to 2004)

Policy/guidance	Key Objectives
Deputy Secretary of Defense Memorandum, August 24, 2000 (No. 4-8460) Subject: DOD CIO Guidance and Policy on GIG Networks	This policy establishes the Defense Information Systems Network (DISN) as DOD's networking capability for the transfer of information in support of military operation in the context of the Global Information Grid (GIG). It further specifies that DISN shall be the means for wide-area and metropolitan-area networking unless granted a waiver through the DISN/GIG waiver board.
Department of Defense Directive 8000.1, February 27, 2002 Subject: Management of DOD Information Resources and Information Technology	This directive establishes policies for DOD information resources management, including information technology, and delineates, authorities, duties, and responsibilities for DOD information resources management activities. It also provides direction on establishing Chief Information Officers at various levels.
Department of Defense Instruction 4630.8, May 2, 2002 Subject: Procedures for Interoperability and Supportability of Information Technology and National Security Systems	This instruction implements an approach that considers both materiel (acquisition or procurement) and nonmateriel (doctrine, organizational, training, leadership, and personnel) aspects to ensure life-cycle interoperability and supportability of information technology and national security systems throughout DOD. It also implements an outcome-based, mission area focused process whereby information technology and national security systems interoperability and supportability requirements for new, modified, and fielded systems are documented, coordinated, implemented, verified, and approved to achieve an integrated, and secure information technology and national security systems infrastructure supporting global operations across the peace-conflict spectrum.
Department of Defense Directive 8100.1, September 19, 2002 Subject: GIG Overarching Policy	The directive states that the GIG shall support all DOD missions with information technology, for national security systems, joint operations, joint task force, and/or combined-task for commands in a manner that offers the most effective, efficient, and assured information handling capabilities available, consistent with national military strategy, operational requirements, and best-value enterprise-level business practices.
Department of Defense Directive 8500.1, October 24, 2002 Subject: Information Assurance	The policy assigns responsibilities to achieve DOD information assurance through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network- centric warfare.
Department of Defense Instruction 8500.2, February 6, 2003 Subject: Information Assurance Implementation	The instructions implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DOD information systems and networks referenced in DOD Directive 8500.1.
Department of Defense Memorandum, July 7, 2003 Subject: End-to-End Information Assurance for the Global Information Grid	The policy establishes a goal to converge voice, video, and data traffic over DOD's inter-network and the National Security Agency (NSA) as lead in developing the information assurance component of the GIG architecture.
Department of Defense Memorandum, September 29, 2003 Subject: Internet Protocol Version 6 (IPv6) Interim Transition Guidance	The policy establishes a goal of transitioning all DOD networking to the next generation of Internet Protocol, IPv6, by fiscal year 2008. As part of this transition, the strategy will be to minimize costs by ensuring products and systems procured, acquired, or in development after October 1, 2003, are capable of operating in IPv6 networks.

Policy/guidance	Key Objectives
Department of Defense, Office of the Chief Information Officer Memorandum, October 24, 2003 Subject: DOD Net-Centric Data Strategy	The policy establishes a DOD-wide goal to institutionalize the practice of identifying all data assets on the GIG by fiscal year 2008. Information will be provided on each data asset to standardize the way data are described and used for all IT and national security systems. This practice will enable DOD to create tools to query data assets across platforms.
Deputy Secretary of Defense Memorandum, November 10, 2003 Subject: GIG Enterprise Services Implementation	The policy establishes a program to begin the development of core enterprise services within the GIG as part of the fiscal year 2006 program review process. Core enterprise services—such as messaging, collaboration, services management, security, discovery, and mediation—are to be developed to provide access and the delivery of data and services across the department.
Chairman of the Joint Chiefs of Staff Instruction CJCSI 6212.01C, November 20, 2003 Subject: Interoperability and Supportability of Information Technology and National Security Systems	This instruction establishes polices and procedures for developing, evaluating and providing interoperability and supportability certification in support of the Joint Capabilities Integration and Development System for acquisition category, nonacquisition category and fielded capabilities.
Chairman of the Joint Chiefs of Staff Instruction CJCSI 3170.01D, March 12, 2004 Subject: Joint Capabilities Integration and Development Systems	This instruction establishes the policies and procedures of the Joint Capabilities Integration and Development System. Procedures established in this instruction support the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council in identifying, assessing, and prioritizing joint military capability needs.
Deputy Secretary of Defense Memorandum, March 22, 2004 Subject: Information Technology Portfolio Management	This policy assigns responsibilities for managing information technology investments as portfolios. It also establishes that decisions on what information technology investments to make, modify or terminate shall be based on architectures, risk tolerance levels, potential returns, outcome goals, and performance.
Department of Defense Directive 8100.2, April 14, 2004 Subject: Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid	This policy assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DOD Global Information Grid. It also directs the development and use of a knowledge management process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout DOD and promotes joint interoperability using open standards throughout DOD for commercial wireless services, devices, and technological implementations.
Department of Defense Directive 4630.5, May 5, 2004 Subject: Interoperability and Supportability of Information Technology and National Security Systems	The directive updates DOD responsibilities for interoperability and supportability of information technology, including national security systems, and implements DOD Chief Information Officer's responsibilities. It also defines a capability-focused, effects-based approach to advance information technology and national security systems interoperability and supportability across DOD and establishes the Net-Ready Key Performance Parameter to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

Sources: DOD (data); GAO (analysis).

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov(202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548