

GAO

Report to the Chairman, Subcommittee
on Military Research and Development
Committee on National Security, House
of Representatives

August 1998

**DEFENSE
INFORMATION
SUPERIORITY**

**Progress Made, but
Significant Challenges
Remain**



**National Security and
International Affairs Division**

B-278201

August 31, 1998

The Honorable Curt Weldon
Chairman, Subcommittee on Military Research
and Development
Committee on National Security
House of Representatives

Dear Mr. Chairman:

In 1996, the Chairman of the Joint Chiefs of Staff issued a conceptual framework for the Department of Defense's (DOD) war fighting called Joint Vision 2010.¹ The document identifies information superiority over the enemy as a key element for the success of this vision. DOD defines information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." DOD believes that information superiority can provide significant advantages over the enemy during a conflict and increase the efficiency of peacetime and wartime operations. However, greater reliance on information systems may also make DOD vulnerable to intrusion and attack on those systems, damaging its war-fighting capability.²

As requested, we evaluated DOD's progress in implementing certain key information superiority activities to provide an indication of how well DOD is progressing toward its information superiority goals. Specifically, you asked us to evaluate DOD's progress in establishing a DOD-wide architecture for the information systems known as Command, Control, Communications, Computers (C4), Intelligence, Surveillance, and Reconnaissance (C4ISR) systems; developing and implementing the Global Command and Control System (GCCS); and establishing the Joint Tactical Radio System (JTRS).

¹Joint Vision 2010 recognizes the need to modernize DOD's war-fighting concepts and respond to advancing technologies for the 21st century. It translates information superiority and the technological advances that are changing traditional war-fighting concepts into new concepts through changes in weapon systems, doctrine, culture, and organization. It also describes the improved intelligence and improved command and control available in the information age as the basis of four operational concepts—dominant maneuver, precision engagement, full dimensional protection, and focused logistics.

²Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996) and Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection (Washington, D.C.: Oct. 1997).

In addition, you asked us to evaluate DOD's progress in implementing recommendations of the Defense Science Board Task Force on Information Warfare-Defense.³ At your request, we reported on DOD's implementation of these recommendations and other activities to protect its C4ISR systems in a separate letter to the Subcommittee for a June 11, 1998, joint hearing with the Military Procurement Subcommittee on the fiscal year 1999 national defense authorization request on Critical Infrastructure Protection-Information Assurance.⁴

Background

Achieving information superiority will be expensive and complex. Based on its analysis of the fiscal year 1999 through 2003 Future Years Defense Plan, DOD estimates it will budget an average of \$43 billion a year (nearly 17 percent of the \$257 billion budget request for fiscal year 1999) for C4ISR systems and activities during the plan period. Achieving information superiority is complex because it involves thousands of decentralized C4ISR systems and information networks. Furthermore, the systems, networks, and information superiority activities are managed by many different offices of the Secretary of Defense, Joint Chiefs of Staff, services, unified commands, and defense agencies throughout DOD.

One of DOD's key activities to achieve information superiority is the development of a Department-wide C4ISR information systems architecture. An information systems architecture is a blueprint that guides and controls the development and maintenance of many related systems. Another key activity is the development and deployment of a Department-wide Defense Information Infrastructure⁵ that features GCCS as DOD's principal worldwide command and control system. GCCS has more capabilities and functions (such as almost real-time knowledge of battlefield conditions, or situational awareness)⁶ than the system it replaced. DOD is also trying to consolidate the services' programmable, modular tactical radio development and acquisition programs into a single JTRS program to

³The recommendations were presented in Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D), Office of the Under Secretary of Defense for Acquisition and Technology (Washington, D.C.: Nov. 1996). The task force determined that DOD's information systems were highly vulnerable to intrusions and attacks and made over 50 recommendations for improving their protection.

⁴DOD's Information Assurance Efforts (GAO/NSIAD-98-132R, June 11, 1998).

⁵DOD describes this infrastructure as all of the information systems and networks used to support the war fighter.

⁶DOD defines situational awareness as knowledge of one's location, the location of friendly and hostile forces, and external factors such as terrain and weather that may affect one's capability to perform a mission.

reduce costs and increase the ability of the services to communicate with each other. JTRS is intended to become one of the Department's key tactical-level C4ISR systems. Finally, DOD is developing and implementing a Department-wide program to protect and defend its C4ISR systems from intrusion and attack; this activity is known as information assurance.

Results in Brief

DOD faces many challenges in achieving its information superiority goals and objectives and may need many years of concerted effort to reach them. One of the key challenges is to complete the development of a C4ISR Architecture, maintain it, and ensure that the many systems that make up the C4ISR infrastructure comply with the Architecture. Without an established architecture and the ability to enforce its use, DOD will find it difficult to make cost-effective development and acquisition decisions and ensure that the systems work with each other, perform as expected, and are adequately protected.

For over 30 years (since 1967) DOD has been trying unsuccessfully to establish some form of Department-wide C4ISR Architecture. In the past 6 years DOD refocused its efforts and made progress by building Department-wide consensus on what should be accomplished by the Architecture and how it should be built. DOD also established the architectural component that defines technical standards for C4ISR systems.

However, the most important component, which defines the information needs that are the basis for setting system standards and acquiring and protecting systems, is not completed. Furthermore, plans for developing and implementing the remainder of the Architecture, to define systems and information flows, are still being formulated. Meanwhile, DOD has been developing a number of critical C4ISR systems and information assurance measures without the benefit of a completed and approved architecture.

Enforcing compliance with the C4ISR Architecture will be an important factor in achieving information superiority. DOD said that compliance with the Architecture will be achieved through a combination of new and existing oversight organizations and processes. For example, DOD recently reorganized the Office of the Assistant Secretary of Defense for C3I to better focus on visibility, support, and responsibility for information technology architectures. It also stated that it will rely on program reviews conducted within traditional planning, budgeting, and acquisition oversight processes to achieve compliance. However, DOD has had

difficulty in achieving compliance with related C4ISR policies and decisions in the past. Therefore, it remains to be seen whether the new organization and traditional oversight processes will be effective in achieving architectural compliance.

DOD's experience with two key C4ISR systems is indicative of the types of challenges ahead. In the absence of a C4ISR architecture, DOD has had mixed success in developing and fielding GCCS, its premier strategic C4ISR system. Although some of its features are well liked by users, GCCS has encountered problems. These include problems with some key functions that cause the system to perform less effectively than expected. It also has potential year 2000 problems that could cause system failure.⁷ Similarly, requirements for JTRS have not been defined in the context of an established C4ISR architecture. Also, DOD officials told us that the Department has suspended development of the JTRS program until Congress approves and funds the program. To meet interim needs, DOD has allowed the services to acquire a limited number of service-unique radios until the joint radios become available.

Progress Made With the Architecture, but Much Work Remains

A single C4ISR architecture is critical for achieving information superiority. After more than 30 years, DOD has begun to make progress toward establishing such an architecture but needs to complete its development, establish adequate information assurance measures, and enforce compliance by the services, unified commands, and agencies.

C4ISR Architecture Is Critical to Achieving Information Superiority

To construct a building it is necessary to have a plan that shows the building's features, its systems and their functions, the way different components interrelate, and the way the components should be built. The architects and engineers must also take into account building codes, rules, and standards. The effective and efficient development and management of an organization's information systems require a similar architectural blueprint. An information systems architecture can be viewed as having both logical and technical components. At the logical level the architecture includes a high-level description of the organizational mission being accomplished, the different functions being performed, the relationships between functions, the information needed to perform these functions, and the flow of information among functions. At the technical level the

⁷Year 2000 problems are difficulties that may be encountered by many information and computer systems that were programmed to use two digits to identify years (98 for 1998), causing a year identified as 00 to be misinterpreted as 1900 instead of 2000 and resulting in program malfunctions or failure.

architecture provides rules and standards to ensure that interrelated systems are interoperable, portable, and maintainable.⁸ These rules and standards include specifications for hardware, software, communication, data, security, and performance characteristics.

DOD is developing, managing, and maintaining an extremely complex system of C4ISR information systems and networks. Establishing an overall architecture under which these information systems and networks will operate is critical for achieving information superiority. Without one, DOD will have difficulty identifying, establishing, and prioritizing (1) the information and information links needed among the services, war fighters, intelligence sources, and national command authorities; (2) the processes and technical standards to be used to communicate information among them; (3) the systems and interoperability needed to achieve the timely transfer of information from where it is maintained to where it is needed; and (4) the measures needed to protect the systems, their information, and the infrastructure supporting them.

Establishing information and information link requirements for conducting operations is particularly important because they are needed to design and develop systems. Information requirements include the amount, type, source, frequency, and speed at which data and information must be gathered, edited, correlated, fused, updated, displayed, printed, and transmitted. Many system developers and program managers have identified ill-defined or incomplete information requirements and requirements growth as root causes of system failure.⁹ Without adequately defined, organizationally approved information requirements, a system may need extensive and costly reengineering before it can become fully operational. For example, we recently reported that the Federal Aviation Administration had to spend over \$38 million to overcome incompatibilities between air traffic control systems, a problem that may have been avoided if the Administration had a complete information systems architecture.¹⁰ System requirements such as security, reliability, availability, and maintainability must be accurately defined because they drive subsequent choices (such as hardware and software) and have a

⁸Interoperable means that systems or programs are capable of exchanging information and operating together effectively. Portable means that a computer program can be transferred from one hardware and/or software configuration to another. Maintainable means that errors in an operational program can be located and fixed with reasonable effort.

⁹Strategic Information Planning: Framework for Designing and Developing System Architectures (GAO/IMTEC-92-51, June 1992).

¹⁰Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, Feb. 3, 1997).

significant impact on system development cost, schedule, and performance.

As for the security provisions of a C4ISR architecture, a March 1997 report of a DOD task force on information assurance stressed the importance of having the architecture drive information assurance.¹¹ The report concluded that adequate information assurance is critical for achieving information superiority and that U.S. forces are at increasing risk of failing in their mission without it. It also concluded that DOD's C4ISR Architecture must support security and that security must be addressed in an integrated way when the system is first designed and not later with add-on products or services. The report further concluded that DOD must provide security links throughout a C4ISR architecture to show what, when, where, and why security should be applied; where, what, and how it will be applied; and the codes and standards for what and how security will be applied.

Past Architecture Efforts Not Successful

DOD has had an official requirement for C4ISR interoperability and for a Department-wide architecture since 1967, when it encountered communications interoperability problems during the Vietnam War. However, it has never adequately met that requirement, even though it experienced similar problems during military operations in Grenada, Panama, and the Persian Gulf. In 1987¹² and again in 1993¹³ we reported that DOD had made little progress in meeting the requirement because it lacked centralized or joint managerial and funding control over individual service priorities, which often took precedence over interoperability priorities. We also reported that all of DOD's component commands, services, and agencies had been unable to agree on what such an architecture should accomplish or what it should consist of.

Recent Progress Made

In 1992, after serious interoperability problems with command, control, communications, computers, and intelligence (C4I) systems in the Persian Gulf War, the Joint Staff began an initiative called C4I for the Warrior to stress joint interoperability, stimulate solutions, and guide the services toward a global information system. This initiative gave stimulus to a

¹¹Improving Information Assurance: A General Assessment and Comprehensive Approach to an Integrated IA Program for the Department of Defense (ASD C3I, Mar. 28, 1997).

¹²Interoperability: DOD's Efforts to Achieve Interoperability Among C3 Systems (GAO/NSIAD-87-124, Apr. 27, 1987).

¹³Joint Military Operations: DOD's Renewed Emphasis on Interoperability Is Important but Not Adequate (GAO/NSIAD-94-47, Oct. 21, 1993).

number of C4ISR development efforts, including the Defense Information Infrastructure, the overall C4ISR Architecture, and the concept of information superiority described in Joint Vision 2010.

Before an effective architecture could be developed, however, DOD had to forge an agreement among the services, commands, and agencies on what that architecture should accomplish and how it would be constructed. Thus, a working group of service, command, and DOD agency representatives in June 1996 established a C4ISR Architecture Framework, which outlined a coordinated, Department-wide approach to C4ISR Architecture development, presentation, and integration. The Framework was updated in December 1997 and agreed on by the services, the Joint Staff, and the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I). According to DOD, the Framework is now required to be used by all DOD organizations.

The Framework describes an overall architecture comprised of three interdependent, interlocking components: an operational, a systems, and a technical subarchitecture. The operational component—known as the Joint Operational Architecture—is supposed to identify and document war-fighting information needs. The system component—known as the Joint Systems Architecture—is supposed to describe which systems, common information flow, and system interfaces will be used to meet war-fighting needs. Finally, the technical component—known as the Joint Technical Architecture—is supposed to specify the characteristics and standards for hardware, software, communications, data, security, and performance.¹⁴ Underlying the building of the information infrastructure and technical subarchitecture was a common operating environment, in which all DOD component organizations would be required to develop, acquire, and deploy C4ISR systems that operate under a common set of standards and protocols to permit interoperability.

The creation of this framework was an important step—it was the first DOD-wide consensus on what a C4ISR architecture should do and how it should be built. The three-part Architecture also conforms to the generally accepted architectural definition described earlier: DOD’s operational subarchitecture corresponds to the logical definition, while the technical

¹⁴In comments on a draft of this report, DOD described the C4ISR Architecture as being comprised of three subarchitectural “views”—the Joint Operational, Joint Technical, and Joint Systems Views. It also used the terms Joint Operational Architecture and Joint Technical Architecture. Because the meaning of the term “view” may be confusing to some readers, we have used only the terms “architecture” or “subarchitecture” when referring to the three architectural components.

and system subarchitectures together correspond to the technical definition.

Multiple DOD organizations are involved in the development of the three-part Architecture. The Joint Staff's C4 Systems Directorate (J6) is responsible for developing the operational subarchitecture, the component services and unified commands are responsible for developing the systems subarchitecture, and the Defense Information Systems Agency (DISA) is responsible for developing the technical subarchitecture. The Office of the Assistant Secretary of Defense for C3I is responsible for overall coordination and integration of the DOD-wide C4ISR Architecture.

Of the three subarchitectures, only the technical subarchitecture has been officially established. In August 1996, DOD completed a first version of the technical subarchitecture and mandated that all new C4ISR systems and major upgrades comply with the standards and guidelines it prescribed. DOD completed a second, expanded version of the technical subarchitecture in February 1998.

Three-Part Architecture and Information Assurance Program Remain Incomplete

Although DOD has established a technical subarchitecture, we believe the operational subarchitecture is the most important of the three subarchitectures and should have been completed first because it determines the basis for information needs, thereby forming the foundation for the other subarchitectures and for determining systems' development and acquisition needs. The operational subarchitecture is still being developed, and DOD officials estimate that its overall structure will be completed in the second quarter of fiscal year 1999. DOD plans to have each unified command develop its own operational architecture and to have a working group under Joint Staff leadership oversee the integration of all the different architectures into a single Joint Operational Architecture. As for the systems subarchitecture, no plans have been set for its development, according to a DOD official.

The need for establishing an overall C4ISR Architecture is highlighted by the architecture's close relationship with information assurance activities. In our June 1998 letter to the Subcommittee on DOD's C4ISR systems protection activities, we noted that DOD's organizations had undertaken a variety of information assurance measures that were not meeting the Department's needs. For example, a DOD internal analysis and a subsequent report in November 1997 concluded that the Department's decentralized information assurance management could not deal with

information assurance adequately because of the proliferation of networks across DOD and that some assurance efforts were only minimally effective.

In our letter we also noted that to improve information assurance management, (1) in December 1997 the Assistant Secretary established an Information Technology Security Certification and Accreditation Process that requires comprehensive information assurance evaluations of all information technology systems in accordance with standard analytical procedures, and (2) in January 1998 the Deputy Secretary directed the Assistant Secretary of Defense for C3I to develop and implement the DOD-wide Defense Information Assurance Program proposed in the November 1997 report. We concluded that the effectiveness of these new activities remains to be determined but also noted that DOD's information assurance efforts are moving forward without a completed and approved C4ISR Architecture in place.

Effective Management Structure to Enforce Compliance Is Essential

Creating the C4ISR Architecture in itself is not enough to build the Defense Information Infrastructure and its attendant systems. An effective management structure to enforce compliance with the Architecture is essential. In December 1996 the Chairman of the Joint Chiefs of Staff, observing that no formal enforcement mechanism existed for the implementation of the C4ISR Architecture Framework, cited the need for a management structure to carry out this task. Specifically, no one had responsibility for enforcing compliance with the Framework. At about the same time, a DOD C4ISR Integration Task Force made a number of recommendations to improve C4ISR management, including a recommendation that DOD establish oversight mechanisms to ensure that the Department's organizations comply with the Architecture Framework.

An example of the sort of problem created by lack of an enforcement mechanism was provided by a Joint Staff biennial assessment of DISA.¹⁵ The assessment found that the services often experienced joint interoperability, connectivity, and configuration management problems with DISA's core program systems after they were fielded. DISA relies on the services at the base, post, station, and camp levels to integrate the systems after they are fielded. The Chairman of the Joint Chiefs of Staff believed that such problems occurred because of so-called "Title 10 concerns"¹⁶ and

¹⁵This biennial assessment is required by 10 U.S.C. Section 193.

¹⁶This phrase refers to the independent funding authority granted the military departments under 10 U.S.C. and a tendency for them to fund their own service-unique requirements before funding joint requirements.

DISA's lack of authority to require the services to adequately fund the integrations needed. The tendency to give individual service requirements higher priority was also noted in a November 1997 DOD Inspector General report,¹⁷ which observed that the sense of urgency or importance of implementing the Joint Technical Architecture is not apparent in the plans and approaches of the Navy and the Air Force, while the Army has shown greater commitment to implementation.

In comments on a draft of this report, DOD indicated that it will rely on a combination of recently established and traditional oversight organizations and processes to achieve compliance with the C4ISR Architecture. These consist of the Architecture Coordination Council, established in 1997 and cochaired by the Under Secretary of Defense for Acquisition and Technology, the Joint Staff's Director for C4 Systems, and the Assistant Secretary of Defense for C3I; the Joint Requirements Oversight Council, supported by requirements analyses provided by a Joint C4ISR Decision Support Center; the Joint Strategic Planning System; the Planning, Programming, and Budgeting System; and the acquisition system. DOD also indicated that it will rely on program reviews conducted within the planning, budgeting, and acquisition oversight processes to achieve compliance with the C4ISR Architecture. Finally, DOD stated that it recently reorganized the Office of the Assistant Secretary of Defense for C3I to better focus on visibility, support, and responsibility for DOD information technology architectures.

It is not yet clear whether these oversight organizations and processes will be effective in achieving compliance with the C4ISR Architecture. As indicated earlier, DOD has had a long history of being unable to override service-unique priorities and establish C4ISR interoperability and a DOD-wide architecture. In addition, other reports we have recently issued on related subjects disclose a similar inability of DOD to attain compliance with C4ISR policies and decisions.¹⁸ Finally, we believe it is too early to gauge the potential impact the reorganization may have on DOD's ability to enforce compliance with the Architecture.

¹⁷Implementation of the DOD Joint Technical Architecture (DOD Inspector General Report No. 98-023, Nov. 18, 1997).

¹⁸For example, Defense IRM: Poor Implementation of Management Controls Has Put Migration Strategy at Risk (GAO/AIMD-98-5, Oct. 20, 1997) and Joint Military Operations: Weaknesses in DOD's Process for Certifying C4I Systems' Interoperability (GAO/NSIAD-98-73, Mar. 13, 1998).

GCCS and JTRS Implementation Efforts Illustrate Challenges Facing DOD

DOD is facing tough challenges in developing and implementing GCCS and JTRS. Although GCCS has greater capabilities and functions—such as almost real-time situational awareness of the battlefield—than its predecessor, the development, fielding, and performance of GCCS have been hampered by fragmented management. DOD is also trying to consolidate the services' programmable, modular tactical radio development and acquisition programs into a single joint radio program to increase interoperability among services and efficiency in acquisition. While awaiting approval and funding of the JTRS Program, the services are procuring interim radios.

GCCS Is an Evolving System

GCCS began as a system of existing command and control components that was to be implemented rapidly to replace DOD's outdated World Wide Military Command and Control System and fulfill the most urgent user requirements. DOD plans to further develop GCCS as an "evolutionary system," which means that DOD will continue to develop its capabilities incrementally as it reacts to user feedback or rapidly evolving new technology. As new GCCS versions are fielded, DOD intends to have added capabilities replace other existing C4ISR systems.

While initially developing GCCS, DOD did not clearly define the system's goals, requirements, and schedules. For example, a 1997 Institute for Defense Analysis report on this evolutionary process said that the GCCS architecture was designed, developed, and fielded not as a single system but through periodic additions of functionality and capability over the past 3 years.¹⁹ It described GCCS as a "set of long-term goals established by DOD senior leadership, the attainment of which does not have a well defined trajectory."

Mixed Success With GCCS

DOD has experienced a mixture of successes and problems in implementing GCCS. For example, users like some of the additional features it provides compared to the old system and found them productive. These features include mission-related communications by e-mail, internet-like web pages, and on-line discussion groups. Users also like the idea of being provided situational awareness of the battlefield. However, some key capabilities, such as the system's operational planning function and the situational awareness function, have experienced problems and are performing less effectively than expected. Also, operator training is deficient, data exchange procedures with coalition partners

¹⁹Richard H. White et al., *An Evolutionary Acquisition Strategy for the Global Command and Control System (GCCS)*, Institute for Defense Analysis (Sept. 1997).

have not been defined, and the system is at risk of failure because year 2000 problems have not been fully resolved. If GCCS encounters year 2000 problems, the United States and its many allies who use GCCS could have difficulty conducting a Desert Storm-type engagement.²⁰ We believe these problems exist partly because DOD does not have a set of clearly defined goals, requirements, and schedules for the system.

GCCS Management Is Fragmented

A May 1995 report by DOD's Office of Inspector General expressed concern about GCCS management and oversight and said that GCCS management is scattered among the Joint Staff, DISA, and the services.²¹ It noted that although DISA is the project manager for GCCS, it does not have the authority to provide overall direction and control of the program. A similar issue was raised in a 1997 study commissioned by DISA on the technical foundation of GCCS.²² That study said that DOD had not established an adequate foundation for enabling full interoperability among DOD computer systems because DISA lacks resources and does not have the formal mission of implementing a complete strategy to achieve interoperability. The study concluded that there is little likelihood of the pieces coming together as envisioned for full interoperability.

DOD recognizes that GCCS needs a more structured acquisition management process and is considering ways to provide this structure, including a strategy proposed in the September 1997 report by the Institute for Defense Analysis. Under this strategy, future GCCS acquisitions would take place in phases so that resources would be applied to meet mission requirements in discrete time periods. Each phase would be controlled by a contract that would describe cost, performance, scheduling, testing, economic, and budgetary issues and identify deliverable command and control capabilities. However, the strategy would still accept the current roles and missions of organizations involved in GCCS.

Establishment of JTRS Program

The Secretary's Defense Planning Guidance for fiscal years 1999-2003 directed the Assistant Secretary of Defense for C3I, in coordination with the Chairman of the Joint Chiefs of Staff and the services, to define

²⁰Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, Apr. 30, 1998).

²¹Management of the Global Command and Control System (DOD Inspector General Report No. 95-201, May 24, 1995).

²²Defense Information Infrastructure Common Operating Environment I&RTS Review and Assessment, prepared by GARTNER Consulting for the Defense Information Systems Agency (Nov. 4, 1997).

DOD-wide requirements for a high-capacity, next-generation, digital, programmable tactical radio. It also directed the Assistant Secretary to establish a joint program for a family of radios that would consolidate similar programs under development by the services—the Army’s Future Digital Radio, the Navy’s Digital Modular Radio, and the Air Force’s Airborne Integrated Terminal.

In response to this directive, DOD officially established the JTRS Program in September 1997.²³ In December 1997, the Under Secretary of Defense for Acquisition and Technology appointed the Army as the program’s permanent component acquisition executive and lead service and directed that a joint program office be established to manage the development of an evolutionary architecture and perform JTRS management functions. According to DOD officials, a joint program manager has been appointed, and the services and the Office of the Secretary have agreed on an organizational structure for the joint program office. However, according to the officials, the activation of the program and joint program office are on hold pending congressional approval of the program and reprogramming action to fund it.

DOD plans to begin fielding JTRS radios between 2002 and 2004. In addition, DOD has established the program’s joint operational requirements but, as with the GCCS and other systems, these have been established without a fully established and approved C4ISR Architecture. To meet interim needs, the services plan to acquire limited numbers of their own radios. The Air Force told us it plans to spend \$133 million for 330 less expensive, reduced capability Airborne Integrated Terminals needed for aircraft operating in Europe to comply with European air traffic control requirements. The Navy told us it plans to spend \$211 million for 352 digital modular radios to comply with a Joint Staff directive to meet Demand Assigned Multiple Access²⁴ standards for satellite communications terminals. The Army told us it plans to begin buying 3,157 radios in fiscal year 2000 to support its digitization program.

The JTRS Program’s objectives are to provide a family of digital, modular, software-programmable radios that will allow military commanders to communicate with their forces through voice, video, or data formats as needed and that will range in configuration from a low-cost joint tactical

²³The program was originally named the Programmable Modular Communications System. It was renamed JTRS in December 1997.

²⁴This is a technology for gaining efficiency in the use of ultra-high frequency satellite communication channels through automated channel sharing by users.

radio to a higher capability, joint multiband, multimode radio. This approach is being used to accommodate the services' many individual requirements, including space and size, and the many different conditions—airborne, ground mobile, fixed station, maritime, and personal communications—in which the radios will be used. The concept is that the radios can be programmed or configured to function in a number of modes and frequencies to fit a user's specific needs. By combining functions and using common components, DOD believes the services will be able to reduce unit costs and the number of radios needed.

Conclusions

DOD faces many challenges in achieving its information superiority goals. These challenges are exemplified by the difficulty DOD has experienced in its efforts to develop and implement the C4ISR Architecture, establish system requirements and operational effectiveness for GCCS, and develop the JTRS Program. DOD's C4ISR architectural and other information superiority activities are complex undertakings and involve considerable investments in C4ISR systems. In addition, they will require overcoming difficult and long-standing institutional problems and organizational boundaries to be successful. Consequently, it may take many years of concerted effort for DOD to reach its information superiority objectives.

DOD's recent efforts to establish a C4ISR Architecture have begun to show progress. However, much work remains to be done. In particular, DOD needs to complete the C4ISR Architecture, follow through with information assurance plans, ensure that efforts resulting from those plans are linked to requirements established by the Architecture, and make certain that established oversight processes are effective in achieving C4ISR systems' compliance with the Architecture. Completion of these activities should enable DOD to make cost-effective decisions for C4ISR systems development and acquisition and make sure that the systems perform as expected.

In our opinion the complexity, magnitude, and cost of DOD's information superiority efforts warrant a comprehensive overview, to be completed annually, of the state of the Department's management and oversight of C4ISR acquisitions. We believe that conveying such an overview, describing to Congress DOD's progress toward achieving a Department-wide C4ISR strategy and compliance with the C4ISR Architecture, would enhance Congress' understanding of this important subject as well as the basis on which decisionmakers consider future C4ISR investment needs.

Recommendations

To enhance DOD's ability to achieve its information superiority goals and objectives, we recommend that the Secretary of Defense (1) establish milestones for completing the C4ISR Architecture and information assurance program and (2) ensure the C4ISR management structure has sufficient authority to enforce compliance with the C4ISR Architecture and is effective in achieving that compliance. A consideration the Secretary should give to achieving that compliance is to ensure that Architecture compliance is incorporated into DOD's planning, programming, and budgeting process and C4ISR systems funding decisions.

Matters for Congressional Consideration

Congress may wish to consider having DOD report, in conjunction with annual budget requests, on the progress being made Department-wide in implementing the information superiority concept and its attendant key C4ISR systems development and acquisitions. In such reports, Congress may wish to require DOD to describe its progress in (1) completing and maintaining the C4ISR Architecture, including progress toward established milestones; (2) establishing information assurance and its compliance with the Architecture; and (3) developing and implementing key C4ISR systems, such as GCCS and JTRS, and the ways and degree to which they are complying with the Architecture and information assurance requirements. Congress also may wish to take DOD's progress into consideration when deliberating the authorization and funding of C4ISR systems. In discussions with us about these suggestions, DOD officials acknowledged that such perspectives are not available and agreed that such information may be useful to Congress and DOD in overseeing C4ISR investments. They stated that DOD is working to establish such perspectives and could modify existing reports to Congress to include them. Rather than establishing a separate reporting requirement, Congress may wish to have DOD modify the reports it already provides to include the information we suggest.

Agency Comments

In commenting on a draft of this report, DOD generally concurred with our recommendations. It also affirmed its commitment to achieving information superiority and stated that it is making significant progress toward that goal. For example, it noted that the Office of the Assistant Secretary of Defense for C3I had recently been reorganized to enhance visibility, support, and responsibility for information technology architectures to achieve information superiority. It also cited the Defense-wide Information Assurance Program as a recent step it has taken to focus attention on the importance of information assurance and to establish a means for achieving that assurance.

DOD agreed with our recommendation that milestones be established for completing the C4ISR Architecture and information assurance program. It also provided additional details on how it plans to complete the development and implementation of the Architecture and Information Assurance Program and pointed out that establishing and maintaining them will be a continuous process involving all levels of the Department. Based on this information, we updated the estimated completion date for the operational subarchitecture. However, DOD did not provide details of how or when the systems subarchitecture would be completed.

DOD also agreed with our recommendation that the Secretary take steps to ensure that an effective management structure is in place with the authority and responsibility to enforce compliance with the C4ISR Architecture. DOD described the oversight organizations and processes it will rely on to achieve compliance with the C4ISR Architecture Framework and its architectures. We incorporated this information and our evaluation of it into the report as appropriate.

DOD also commented on our matters for congressional consideration. DOD stated that it already provides information to Congress on the Department's progress toward milestones through documents such as congressional justification books for C4ISR programs, which are submitted in conjunction with annual oversight hearings. In reviewing the documents referred to by DOD, we found that they do not provide a comprehensive overview of the progress DOD is making, Department-wide, on the C4ISR Architecture and on C4ISR systems within the context of the Architecture and information superiority goals. In further discussions with DOD officials about these matters, the officials acknowledged that such a Department-wide perspective is not available and agreed that such information may be useful to Congress and DOD in overseeing C4ISR investments. They stated that DOD is working to establish such perspectives. However, these officials also stated that they were concerned that our suggestion of the matters for congressional consideration would require an additional reporting mechanism separate from annual budget submissions and believed existing reports to Congress could be modified to provide the information. We have clarified that the congressional reporting we are suggesting could be done within the context of existing reports.

Scope and Methodology

To determine the progress of DOD's efforts in establishing an overall C4ISR Architecture, we obtained and reviewed the initial documents and latest

drafts of DOD's C4ISR Architecture Framework and Joint Technical Architecture. To evaluate the issues DOD faces in implementing the framework, we reviewed its C4ISR Integration Task Force Executive Report (Dec. 23, 1996) and the Joint Chiefs of Staff's Combat Support Agency Review of the Defense Information Systems Agency (Dec. 30, 1996). To confirm our analysis of these documents and to determine the latest progress in implementing a DOD-wide C4ISR Architecture, we interviewed senior officials of the headquarters offices of the Assistant Secretary of Defense for C3I; the C4I Integration Support Activity, including the Director and Deputy Director; and the Joint Staff, including the Director for C4 Systems. We also relied on our previous reports on DOD's C4I interoperability efforts for our analysis of DOD's past architectural efforts. In addition, we relied on information in our separate June 11, 1998, letter to the Subcommittee concerning DOD's information assurance efforts for perspectives on these efforts. The scope and methodology of our efforts for that work are contained in the letter.

To determine the progress of GCCS, we reviewed relevant reports, briefings, and other documents from and interviewed appropriate officials within the headquarters offices of the Assistant Secretary of Defense for C3I; the Joint Staff; DISA's GCCS program office; and the Army, Navy, Marine Corps, and Air Force. We also interviewed and received briefings from appropriate officials and reviewed relevant program documents during visits to the U.S. Atlantic Command and U.S. Central Command with respect to the commands' experiences with GCCS and users' points of view on its development and progress. In addition, we observed the use of GCCS in Unified Endeavor 98-1, a simulated joint task force war-game exercise at the U.S. Atlantic Command's Joint Training, Analysis, and Simulation Center in Suffolk, Virginia; in the U.S. Central Command war room; and in the Army's Task Force XXI Advanced Warfighting Experiment in Fort Hood, Texas. We also reviewed relevant studies and reports from the Defense Science Board, the DOD Inspector General, and the Institute for Defense Analysis. Finally, we interviewed a former Assistant Secretary of Defense for C3I and a former DISA director who were involved in GCCS conceptualization, development, and initial implementation. At the time of our interviews, these two officials held executive positions with DOD information technology contractors.

To determine DOD's progress in developing and implementing JTRS, we interviewed appropriate JTRS program officials within the headquarters offices of the Assistant Secretary of Defense for C3I; the Under Secretary of Defense (Comptroller); and the Army, Navy, and Air Force. We reviewed

relevant correspondence, cost and schedule data, and other documents pertaining to the JTRS program.

In addition to the work described above, we sought perspectives on information superiority implementation management in general through interviews with a former Assistant Secretary of Defense for C3I; a panelist and several staff members responsible for C4ISR issues on the National Defense Panel; a former Joint Staff C4 Systems and DISA director; and staff members of a National Research Council of the National Academy of Sciences review of Department of Defense C4I programs. We received briefings and reviewed relevant documents from appropriate senior and other officials within the headquarters offices of the Assistant Secretary of Defense for C3I, including the Deputy Assistant Secretary of Defense for C3 and the Director and Deputy Director of the C4I Integration Support Activity; DISA; and the Joint Staff, including the Director for C4 Systems. We also obtained and reviewed relevant studies and reports from the Congressional Research Service, Defense Science Board, DOD Inspector General, Institute for Defense Analysis, and National Defense Panel.

We performed our review from July 1997 to June 1998 in accordance with generally accepted government auditing standards.

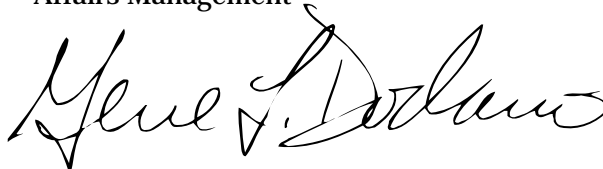
We are sending copies of this report to the Ranking Minority Member of the Subcommittee; the Chairman and Ranking Minority Member of the House Committee on National Security; other interested congressional committees; and the Secretaries of Defense, the Army, the Navy, and the Air Force. We will also make copies available to others upon request.

This report was prepared under the direction of Allen Li, Associate Director, Defense Acquisitions Issues, National Security and International Affairs Division, and Jack L. Brock, Jr., Director, Governmentwide and

Defense Information Systems Issues, Accounting and Information Management Division. Please contact Mr. Li on (202) 512-4841 if you or your staff have any questions concerning this report. Other major contributors to the report are listed in appendix II.



Henry L. Hinton, Jr.
Assistant Comptroller General
National Security and International
Affairs Management



Gene L. Dodaro
Assistant Comptroller General
Accounting and Information

Contents

Letter		1
Appendix I		22
Comments Provided	GAO Comments	28
by the Department of		
Defense		
Appendix II		30
Major Contributors to	Accounting and Information Management Division	30
This Report		

Abbreviations

C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
DISA	Defense Information Systems Agency
DOD	Department of Defense
GCCS	Global Command and Control System
IA	Information Assurance
JTRS	Joint Tactical Radio System

Comments Provided by the Department of Defense

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000



July 29, 1998

Mr. Henry L. Hinton
Assistant Comptroller General
National Security and
International Affairs Division
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Hinton:

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) draft, 'INFORMATION SUPERIORITY: Progress Made, But Significant Implementation Issues Still Need Resolution,' dated July 6, 1998 (GAO Code 707294/OSD Case 1646).

The DoD generally concurs with the GAO recommendations with comments (enclosure). A number of efforts are already underway to improve the Department's process of achieving Information Superiority.

The DoD is firmly committed to achieving information superiority and is making significant progress toward achieving that goal. The recent reorganization of the office of the ASD(C3I) was directed at better focusing the Department's support to achieve Information Superiority as described in Joint Vision 2010. The reorganization will also provide enhanced visibility and development of the DoD-wide Information Technology (IT) Architecture directed by the Information Technology Management Reform Act (ITMRA). In recognition that Information Superiority is not limited to the functions assigned to the OASD(C3I) and must also include all DoD functional domains, the reorganization provides a clear focal point and responsibility for DoD-wide IT architectures under the Deputy Chief Information Officer.

With respect to the GAO suggestion that DoD prepare an annual report to Congress to assess its progress in meeting the established milestones, DoD annually prepares the Congressional Justification Books (CJB) and Congressional Budget Justification Books (CJB) for C4ISR programs which DoD believes makes the information readily available. Additionally, the DoD architecture products are routinely made available upon request to congressional staff members to provide further information.




See comments 1 and 5.

See comment 2.

Appendix I
Comments Provided by the Department of
Defense

The DoD appreciates the opportunity to comment on the GAO draft report. Technical comments have been provided separately to enhance the accuracy of the GAO report. The point of contact for this report is Mr. John Osterholz, (703) 607-0231, Director, Information Integration and Interoperability.

Sincerely,



Arthur L. Money
Senior Civilian Official

**GAO DRAFT REPORT DATED JULY 6, 1998
(GAO CODE 707294/OSD Case 1646)**

**“INFORMATION SUPERIORITY: PROGRESS MADE, BUT SIGNIFICANT
IMPLEMENTATION ISSUES STILL NEED RESOLUTION”**

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense take steps to ensure that milestones are established for completing the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) architecture and information assurance program.

DOD RESPONSE: Concur. The Department agrees that milestones for completing the C4ISR Architecture and the Information Assurance Programs must be established.

It should be understood that in referring to the DoD C4ISR Architecture, one is actually referring to three sub-Architectural views: the Joint Operational View, the Joint Technical View, and the Joint Systems View. These views ultimately provide the content and products supporting C4ISR acquisition decisions. The establishment and maintenance of the architecture views is a continuing process that involves all levels within the Department.

The J-6, on behalf of the Joint Staff, accepted an assignment from the Architecture Coordination Council (ACC) to develop a Joint Operational Architecture (JOA) describing the Joint Operational View of the DoD's C4ISR domain. In its fullest realization, the JOA would describe all the information processing requirements and information exchange requirements generated by the activities of our warfighting forces, and the sensors supporting them. Ultimately, the scope will span from the National Command Authority to the “foxhole”, for all CINCs, all appropriate missions, and all applicable levels of conflict as they are projected into the out years.

In 1998, the Joint Battle Center and the Information, Integration and Interoperability Directorate within the OASD (C3I) embarked on a collaborative effort to broaden the current Joint Staff approach toward the development of this Joint Operational Architecture (JOA) and to address the full range of requirements necessary to establish Information Superiority at the operational level of the Joint Forces Commanders (JFCs). This architecture, which must embrace our evolving National Military Strategy, changing geo-political threats, emerging Joint doctrine, and the subsequent tactics, techniques, and procedures (TTPs) used by our warfighters will be a “living” document, always changing, and always requiring update. Because of its dimensionality, it will be enormous in scope, breadth, and depth.

The approach taken in the development of the JOA must be bi-directional: (1) an overarching “top down” view must be taken in order to develop its required data structure and to ensure adherence to DoD data models and standards. This structure must be thought out and defined from the highest national levels down to the lowest tactical levels, with consistency

See comment 3.

Appendix I
Comments Provided by the Department of
Defense

across all our Services, and must include the presence and influence of coalition partners as well; (2) Due to the limits in fiscal and personnel resources, it will be "populated" incrementally by development of prioritized sub-JOAs for specific CINCs, corresponding to specific JFC missions within given conflict scenarios. Given the magnitude and scope of this undertaking, and the coordination required, DoD estimates that the initial overall structure can be completed within FY 2000. Populating this structure will require development of many sub-JOAs, which can be developed in parallel. Depending on the resources available, the particular JFC scenarios selected, and the size and complexity of the CINC's Area of Responsibility (AOR), each will require from 6-12 months.

In concert with this effort, ASD (C3I) has been actively working with the Unified Commands to develop appropriate C4ISR architectures for their areas of responsibility. "High-level" Command C4ISR Architectures (CCA) were developed in all Unified Commands during 1997-1998. An effort is currently underway with USCENTCOM to develop a detailed Command and Control (C2) Architecture. This C2 architecture will be used as a prototype for the other Unified Commands. A baseline for this architecture will be completed in 1998. The objective architecture is expected to be completed during the second quarter of FY99.

Building on the prototype architecture, OASD (C3I) has defined the C4ISR Architectures for the Warfighter (CAW) Program which is an evolution of the long-standing C4ISR Integrated Architecture Program (CIAP). The CAW program calls for the development in each Unified Command, during the 1999 - 2000 timeframe, of a detailed Command and Control (C2) Architecture; Intelligence, Surveillance, and Reconnaissance (ISR) Architecture; and a Computer and Communications Infrastructure Architecture (CCIA). Each Unified Command's high-level CCA encapsulates and summarizes the C2, ISR, and CCIA architectures. The CCIA documents the physical description of the sensors, processing platforms, databases, software applications, and communications assets available within the Command, and provides the basis for cross-Command assessments which will be performed to identify issues common across multiple Unified Commands.

In addition to the C4ISR architectures being developed within the Unified Commands, the Services and Defense Agencies are moving toward development of C4ISR architectures according to the C4ISR Architecture Framework. The development and composite of these architectures represent an important and essential step in defining and understanding DoD's C4ISR environment.

As noted by GAO, the DoD has taken recent steps to focus attention on the importance of Information Assurance (IA). The Department's IA objective is to continuously provide for the availability, integrity, authentication, confidentiality, non-repudiation, and the rapid restoration of mission essential elements of the DII. Critical to achieving this objective is the implementation of a DoD-wide planning and integration framework. To that end, on January 30, 1998, the Deputy Secretary of Defense, approved the creation of the Defense-wide Information Assurance Program (DIAP). The recommendations for the DIAP are the result of efforts of broad IA community participation over the past several years, including:

See comment 4.

**Appendix I
Comments Provided by the Department of
Defense**

- the October 9, 1996 Program Decision Memorandum II (PDM II) directed assessment conducted by the Department-wide Information Assurance Task Force, and
- the August-September 1997 IA Integrated Process Team (IA IPT) effort directed by Secretary of Defense memorandum of August 12, 1997.

The recommendations reflect the increasing understanding across the Department that IA is an operational readiness issue and that increasing dependence on inter-networked systems and services creates a *shared risk* environment necessitating an unprecedented level of coordination and unity of effort across the Department. The DIAP will provide the common management framework and central oversight necessary to ensure the protection and reliability of the DII. While planning and integration will be centralized, execution of individual Component programs will remain the responsibility of the Components. Also necessary is the building of a culture among all the Department's Components in which IA is recognized and valued.

Accordingly, the DIAP will continuously compare DoD's IA programs and functions against its operational and business information requirements, Defense-wide readiness standards, and threats to the DII; it will infuse IA throughout the Department's operations as a fundamental element of readiness and training. Operational readiness standards will be used to assess the adequacy of the protection afforded to the Department's information, information systems, networks, and the entire DII. This effort will provide a comprehensive and real-time picture of the DoD's IA programs. It will enable DoD to accurately develop, validate, and prioritize DoD-wide IA requirements, determine the return on its IA investments, and objectively assess its efforts to protect the DII.

The transformation of IA from a largely technical issue to an operational imperative is critical to the success of the Department's IA strategy. The DIAP will constitute a significant management, organizational, and cultural change within the Department. It will ensure that DoD's IA programs extend beyond traditional Service perspectives to meet the growing challenges of a dynamic global information environment. Through this process, the Department will be able to leverage information and rapidly infuse information technology to enhance the efficiency of its business activities and the impact of its military operations.

The DIAP achieved an Initial Operating Capability (IOC) milestone in June 1998. A Senior DIAP Steering Group, composed of flag officers representing the Services, Defense Information Systems Agency (DISA), Joint Staff, and National Security Agency (NSA) was chartered to provide strategic guidance and direction. The DIAP Staff Director, senior Team Leaders, and core staff are on board working the detailed planning for near, mid and long-term milestones.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense take steps to ensure that an effective management structure is in place with the authority and responsibility for enforcing compliance with the C4ISR architecture when funding C4ISR systems development, acquisition, and support activities.

Appendix I
Comments Provided by the Department of
Defense

DOD RESPONSE: Concur. In line with this GAO recommendation, the Architecture Coordination Council (ACC) was created in 1997. Co-chaired by the Under Secretary of Defense for Acquisition and Technology (USD(A&T)), the Joint Staff represented by J-6 Director, Command, Control, Communications and Computer Systems and the Assistant Secretary of Defense (C3I), the ACC ensures that architectures developed in DoD and the Intelligence Community comply with the C4ISR Architecture Framework and are properly inter-linked in a system-of-systems context. The ACC's business strategy is designed to ensure that DoD IT efforts will result in improved operational effectiveness and information integrity with a consistent, coherent, interoperable system-of-systems. The ACC facilitated the approval of the Joint Technical Architecture (JTA), Version 2.0, on February 23, 1998 which extends the applicability of standards and specifications beyond tactical C4ISR to encompass modeling and simulation; base, post, camp and station sustainment systems and weapon systems and platforms. On the same date, the ACC ratified the C4ISR Architecture Framework, Version 2.0, and mandated its use by all elements within DoD. This represents a significant increase in scope for DoD architecture activities and recognizes that interoperability follows information flow from end-to-end. In addition to overseeing future versions of the JTA, the ACC is facilitating the development of a Joint Operational Architecture and is currently considering a concept of integration for major program systems architectures.

See comment 5.

Additionally, in 1996 the DoD established the Joint C4ISR Decision Support Center (DSC). The DSC conducts analysis of C4ISR requirements for acquisition decision-makers to ensure that DoD fields only those C4ISR components that will lead to an integrated system of systems for joint and combined operations. The activities of the DSC are overseen by a senior steering group composed of the USD (A&T), the Vice-Chairman of the Joint Chiefs of Staff and the Assistant Secretary of Defense (C3I). The recommendations of the DSC are provided to the Joint Requirements Oversight Council (JROC). To date, the activities of the DSC have led to development of a joint, integrated sensor and communications systems architecture, often referred to as "Sensor to Shooter".

See comment 5.

Enforcing compliance with the guidance of the ACC and the C4ISR Architectural Framework will be accomplished through the DoD's Joint Strategic Planning System (JSPS), the Planning, Programming and Budgeting System (PPBS) and the Acquisition System, similar to the current enforcement of the JTA. Compliance with the JTA is enforced through a process of program and cross-program reviews conducted by OASD (C3I), the Joint Staff and USD (A&T) as the various programs progress through the system development and acquisition process. Specific enforcement mechanisms will expand and take advantage of control points embedded within JSPS, PPBS, and the Acquisition System.

See comment 5.

The following are GAO's comments on the Department of Defense's (DOD) letter dated July 29, 1998.

GAO Comments

1. We have incorporated discussions of the reorganization into the report.
2. In discussions with DOD officials about these statements, the officials said that DOD was referring specifically to the Congressional Justification Book for Command, Control, and Communications; Information Technology Exhibit for the budget submission (Exhibit 43); three volumes of congressional justification books on joint military and tactical intelligence programs and related activities; congressional budget justification books submitted by the Director of Central Intelligence on national intelligence programs; and Command C4ISR Architectures produced by each unified command. However, we reviewed these documents (with the exception of the national intelligence-related document, which has restricted access) and did not find the comprehensive overview of DOD's C4ISR systems that we think would enable Congress to fully understand and oversee the Department's information superiority-related authorization and funding requests.

For example, these submissions do not provide a Department-wide overview of DOD's progress in developing, implementing, and achieving compliance with the C4ISR Architecture; compliance is a key to achieving and managing information superiority effectively and efficiently. In addition, the documents do not provide sufficient information about (1) how the various C4ISR systems for which authorizations and funding have been requested comply with the Architecture, (2) how the C4ISR systems relate to one another in the overall scheme of the C4ISR Architecture (providing a perspective on potential system redundancies and relative need), or (3) how and to what extent the systems comply with information assurance requirements dictated by the Architecture and DOD's Defense-wide Information Assurance Plan.

Currently, the information provided by DOD is scattered among multiple and voluminous documents. Although we did not assess the usefulness of these documents for other purposes, such as command-wide guidance to system developers that may be provided by the command architectures, we found that they do not provide a comprehensive overview of the progress DOD is making, Department-wide, on the C4ISR Architecture and on C4ISR systems within the context of the Architecture and information superiority goals. For example, congressional justification books

summarize progress of individual systems. In subsequent discussions with DOD officials on the content and purpose of the documents referred to by DOD, the officials acknowledged that a Department-wide perspective is not available and agreed that such information may be useful to Congress and DOD in overseeing C4ISR investments. They stated that DOD is working to establish such perspectives. However, these officials also stated that they were concerned that our suggestion of the matters for congressional consideration would require an additional reporting mechanism separate from annual budget submissions and believed existing reports to Congress could be modified to provide the information. We recognize that current DOD reports to Congress could form a viable framework within which to incorporate our suggestion for a Department-wide overview and progress description. Consequently, we have clarified that the congressional reporting we suggest could be accomplished within the context of existing reports.

3. DOD continues to use the terms Joint Operational Architecture, Joint Technical Architecture, and Joint Systems Architecture in conjunction with the terms Joint Operational View, Joint Technical View, and Joint Systems View. We believe the use of both sets of terms may be confusing to some readers. Consequently, we have used only the terms “architecture” or “subarchitecture” when referring to the three architectural components in this report.

4. Based on the information provided, we updated the estimated completion date for the operational subarchitecture. However, DOD did not provide details of how and when the systems subarchitecture would be developed and completed. Therefore, it remains to be seen how DOD will develop and implement this portion of the Architecture.

5. We incorporated information DOD provided on Architecture compliance mechanisms and recognized the reorganization initiatives. As stated in the report, it is not yet clear whether these mechanisms and the reorganization will be effective in achieving compliance. For example, DOD has a long history of being unable to use its review processes effectively to overcome service-unique priorities and attain compliance with policies and decisions in joint C4ISR systems matters. While the organizational changes may enhance DOD’s success in achieving architectural compliance, we believe it is too early to gauge their potential effectiveness in this regard.

Major Contributors to This Report

National Security and International Affairs Division

Charles F. Rey, Assistant Director
Charles R. (Randy) Climpson, Evaluator-in-Charge
Robert R. Hadley, Senior Evaluator
Gregory K. Harmon, Senior Evaluator
Bruce H. Thomas, Senior Evaluator
Stefano Petrucci, Communications Analyst

Accounting and Information Management Division

Keith A. Rhodes, Technical Director
Joseph T. (Mickey) McDermott, Assistant Director
Joseph A. DeBrosse, Senior Evaluator

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

<http://www.gao.gov>

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

