United States General Accounting Office

GAO

Report to the Chairman,
Committee on Armed Services,
House of Representatives

March 2003

DEFENSE ACQUISITIONS

Steps Needed to Ensure Interoperability of Systems That Process Intelligence Data

GAO-03-329

March 2003

DEFENSE ACQUISITIONS

Steps Needed to Ensure Interoperability of Systems That Process Intelligence Data

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-329, a report to the Chairman, Committee on Armed Services, House of Representatives

Why GAO Did This Study

Making sure systems can work effectively together (interoperability) has been a key problem for the Department of Defense (DOD) yet integral to its goals for enhancing joint operations. Given the importance of being able to share intelligence data quickly, we were asked to assess DOD's initiative to develop a common ground-surface-based intelligence system and to particularly examine (1) whether DOD has adequately planned this initiative and (2) whether its process for testing and certifying the interoperability of new systems is working effectively.

What GAO Recommends

GAO recommends that DOD enhance its planning to include a detailed migration plan and schedule. GAO also recommends that DOD take steps needed to enforce its process and determine why the services are slow to certify systems in order that it can implement controls and incentives needed to spur compliance. DOD generally agreed with our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-03-329.

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

What GAO Found

DOD relies on a broad array of intelligence systems to study the battlefield and identify and hit enemy targets. These systems include reconnaissance aircraft, satellites, and ground-surface stations that receive, analyze, and disseminate intelligence data. At times, these systems are not interoperable—either for technical reasons (such as incompatible data formats) and/or operational reasons. Such problems can considerably slow down the time to identify and analyze a potential target and decide whether to attack it.

One multibillion-dollar initiative DOD has underway to address this problem is to pare down the number of ground-surface systems that process intelligence data and upgrade them to enhance their functionality and ensure that they can work with other DOD systems. The eventual goal is an overarching family of interconnected systems, known as the Distributed Common Ground-Surface System (DCGS).

To date, planning for this initiative has been slow and incomplete. DOD is developing an architecture, or blueprint, for the new systems as well as an overarching test plan and an operational concept. Although DCGS was started in 1998, DOD has not yet formally identified which systems are going to be involved in DCGS; what the time frames will be for making selections and modifications, conducting interoperability tests, and integrating systems into the overarching system; how transitions will be funded; and how the progress of the initiative will be tracked.

Moreover, DOD's process for testing and certifying that systems will be interoperable is not working effectively. In fact, only 2 of 26 DCGS systems have been certified as interoperable. Because 21 of the systems that have not been certified have already been fielded, DOD has a greater risk that the new systems will not be able to share intelligence data as quickly as needed. Certifications are important because they consider such things as whether a system can work with systems belonging to other military services without unacceptable workarounds and whether individual systems conform to broader architectures designed to facilitate interoperability across DOD.

Examples of Ground-Surface Systems Involved in DCGS

Navy system that allows shipboard operators to monitor and analyze signals intelligence

Remote Army system that processes and analyzes data from a variety of intelligence collecting sources on the battlefield

Centralized military facilities that receive and transmit data and imagery from reconnaissance aircraft, radar systems, satellites

Source: GAO.

Contents

Abbreviations

C4SIR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
DCGS	Distributed Common Ground-Surface System
JITC	Joint Interoperability Test Command

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

March 31, 2003

The Honorable Duncan Hunter
Chairman, Committee on Armed Services
House of Representatives

Dear Mr. Chairman:

The Department of Defense (DOD) relies on a broad array of intelligence systems to study the battlefield and to identify and hit enemy targets. These systems include reconnaissance aircraft, satellites, and ground-surface-based stations that receive, analyze, and disseminate intelligence data. A key problem facing DOD is the inability of these systems to operate effectively together for technical reasons (such as incompatible data formats) and/or operational reasons. Such problems can considerably slow the time involved with identifying and analyzing a potential target and deciding whether to attack it, as well as delivering an order to the war fighter in charge of the attack.

DOD recognizes this problem, and it has undertaken a range of initiatives aimed at improving interoperability among all of its systems. One multibillion-dollar initiative underway since 1998 is to pare down the number of ground-surface systems that process intelligence data and upgrade them to enhance their functionality and to ensure that they are interoperable with other DOD systems. The eventual goal is the migration to an overarching, interconnected family of systems for processing intelligence data known as the Distributed Common Ground-Surface System (DCGS). Given the importance of the DCGS initiative to the war fighter, you asked us to assess (1) whether DOD has adequately planned for these processing systems and (2) whether DOD's process for testing and certifying the interoperability of the systems is working effectively.

Results in Brief

DOD has not completed plans for its initiative to pare down and enhance its ground-surface-based systems for processing intelligence data. DOD is developing an architecture, or blueprint, for the new systems, but it has not yet formally identified which systems are to be involved in the migration initiative; what the time frames will be for making selections and modifications, conducting interoperability tests, and integrating systems into the overarching system; how the transitions will be funded; and how the success of the initiative will be tracked. For example, DOD has not completed an overarching test plan that would define when and how

interoperability tests will be conducted. Given the range of disparate interests among the services and the billions of dollars involved, such plans are critical to ensuring that the migration is adequately funded and managed.

Moreover, DOD's process for testing and certifying that ground-surface-based processing systems will be interoperable is not working effectively. In fact, only 2 of 26 DCGS systems have been certified as interoperable. Because 21 of the systems that have not been certified have already been fielded, there is greater risk that the systems cannot share data as quickly as needed. Moreover, while certifications are planned for 17 of the 26 systems, they are not planned for 7 others. The certification process is important because it considers such things as whether systems can work with systems belonging to the other military services without unacceptable workarounds or special interfaces, whether they are using standard data formats, and whether they conform to broader architectures designed to facilitate interoperability across DOD. One reason why the process is not working effectively is the incomplete planning discussed above, including the lack of an overarching test plan. Other reasons cited by DOD officials are that system managers are more focused on getting systems fielded quickly and/or they do not want to fund the certification process, as DOD requires them to do. Our work has also shown that the military services focus more on meeting their own requirements when developing new systems as opposed to requirements that would facilitate operating jointly with other services.

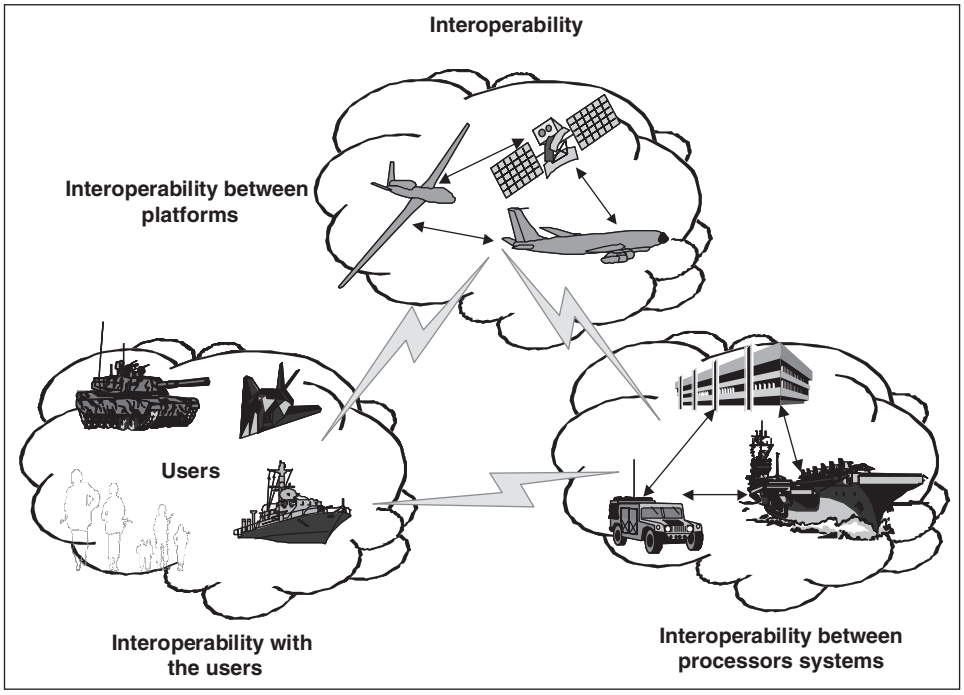
We are making recommendations that DOD enhance its planning to include a detailed migration plan and schedule. We are also recommending that DOD take steps needed to enforce its certification process and determine why the services are slow to certify their systems in order that it can implement the controls and incentives needed to spur compliance. DOD generally agreed with our recommendations.

Background

The military services and defense agencies, such as the National Security Agency and the National Imagery and Mapping Agency, collect and use intelligence data—either in the form of photographic, radar, or infrared images or electronic signals—to better understand and react to an adversary's actions and intentions. This data can come from aircraft like the U-2 or Global Hawk or satellites or other ground, air, sea, or spaced-based equipment. The sensors that collect this data are linked to ground-surface-based processing systems that collect, analyze, and disseminate it

to other intelligence processing facilities and to combat forces. (See figures 1 and 2.) These systems can be large or small, fixed, mobile, or transportable. For example, the Air Force operates several large, fixed systems that provide extensive analysis capability well beyond combat activities. By contrast, the Army and Marine Corps operate smaller, mobile intelligence systems that travel with and operate near combat forces.

Figure 1: Illustration of Equipment and Platforms That Need to Be Interoperable



Source: GAO.

Figure 2: Examples of Ground-Surface-Based Systems for Processing Intelligence Data

- The Air Force's Deployable Shelterized System, which processes and analyzes data collected by U-2 aircraft.
- The Navy's ship signals exploitation equipment, which allows shipboard operators to monitor and analyze signals intelligence.
- The Army's All Source Analysis System Remote Work Station, which processes and analyzes information from a variety of sources on the battlefield.
- The Marine Corps Common Ground Station, which receives and processes intelligence data from surveillance aircraft and radar systems.

Source: GAO.

A key problem facing DOD is that these systems do not always work together effectively, thereby slowing down the time it takes to collect data and analyze and disseminate it sometimes by hours or even days, though DOD reports that timing has improved in more recent military operations. At times, some systems cannot easily exchange information because they were not designed to be compatible and must work through technical patches to transmit and receive data. In other cases, the systems are not connected at all. Compounding this problem is the fact that each service has its own command, control, and communications structure that present barriers to interoperability.

Among the efforts DOD has underway to improve interoperability is the migration to a family of overarching ground-surface systems, based on the best systems already deployed and future systems. DCGS will not only connect individual systems but also enable these systems to merge intelligence information from multiple sources. The first phase of the migration effort will focus on connecting existing systems belonging to the military services—so that each service has an interoperable "family" of systems. The second phase will focus on interconnecting the families of systems so that joint and combined forces can have an unprecedented, common view of the battlefield. DOD's Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence is leading this effort.

Successfully building a compatible ground-surface system is extremely challenging. First, DOD is facing a significant technical challenge. The ground-surface-based systems must not only have compatible electronic connections, but also compatible data transfer rates and data formats and vocabularies. At the same time it modifies systems, DOD must protect sensitive and classified data and be able to make fixes to one system without negatively affecting others. All of these tasks will be difficult to achieve given that the systems currently operated were designed by the individual services with their own requirements in mind and that they still own the systems. Second, sufficient communications capacity (e.g., bandwidth) must exist to transmit large amounts of data. DOD is still in the early stages of adding this capacity through its bandwidth expansion program. Third, DOD must have enough qualified people to analyze and exploit the large volumes of data modern sensors are capable of collecting. Lastly, DOD must still address interoperability barriers that stretch well beyond technical and human capital enhancements. For example, the services may have operating procedures and processes that simply preclude them from sharing data with other services and components, or they may have inconsistent security procedures. Formulating and following common processes and procedures will be difficult since the services have historically been reluctant to do so.[1]

Planning for Migration Effort Is Incomplete

Given the multi-billion-dollar commitment and many technical and operational challenges with the migration initiative, it is critical that DOD have effective plans to guide and manage system development. These would include such things as a comprehensive architecture, migration plan, and investment strategy. However, even though it initiated DCGS in 1998 and is fielding new intelligence systems, DOD is still in the beginning stages of this planning. It is now working on an enterprise architecture, a high level concept of operations for the processing of intelligence information, and an overarching test plan, and it expects these to be done by July 2003. DOD has not yet focused on an investment strategy or on a migration plan that would set a target date for completing the migration and outline activities for meeting that date. By fielding systems without completing these plans, DOD is increasing the risk that DCGS systems will not share data as quickly as needed by the warfighter.

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

Planning Elements Essential to Success of DOD's Migration Effort

Successfully moving toward an interoperable family of ground-surface-based processing systems for intelligence data is a difficult endeavor for DOD. The systems now in place are managed by many different entities within DOD. They are involved in a wide range of military operations and installed on a broad array of equipment. At the same time, they need to be made to be compatible and interoperable. DOD's migration must also fit in with long-term goals for achieving information superiority over the enemy. Several elements are particularly critical to successfully addressing these challenges. They include an enterprise architecture, or blueprint, to define the current and target environment for ground-based processing systems; a road map, or migration plan to define how DOD will get to the target environment and track its progress in doing so; and an investment strategy to ensure adequate resources are provided toward the migration. Each of these elements is described in the following discussions.

- *Enterprise architecture*. Enterprise architectures systematically and completely define an organization's current (baseline) or desired (target) environment. They do so by providing a clear and comprehensive picture of a mission area—both in logical (e.g., operations, functions, and information flows) terms and technical (e.g., software, hardware, and communications) terms. If defined properly, enterprise architectures can assist in optimizing interdependencies and interrelationships among an organization's operations and the underlying technology supporting these operations. Our experience with federal agencies has shown that attempting to define and build systems without first completing an architecture often results in systems that are duplicative, not well integrated, and unnecessarily costly to maintain and interface, and do not optimize mission performance.[2] DOD also recognizes the importance of enterprise architectures and developed a framework known as the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework for its components to use in guiding efforts similar to DCGS. DOD's acquisition guidance also requires the use of architectures to characterize interrelationships and interactions between U.S., allied, and coalition systems.[3]

[2] U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use across the Federal Government Can Be Improved*, GAO-02-6 (Washington, D.C.: Feb. 2002).

[3] Department of Defense, *C4ISR Architect Framework* (Washington, D.C.: Dec. 1997).

- *Migration plan or road map.* Given the size and complexity of DCGS, it is important that the migration be planned in convenient, manageable increments to accommodate DOD's capacity to handle change. At a minimum, a plan would lay out current system capabilities, desired capabilities, and specific initiatives, programs, projects, and schedules intended to get DOD and the services to that vision. It would also define measures for tracking progress, such as testing timeliness and the status of modifications, roles and responsibilities for key activities, and mechanisms for enforcing compliance with the migration plan and ensuring that systems conform to technical and data standards defined by the architecture. Such plans, or road maps, are often developed as part of an enterprise architecture.

- *Investment strategy.* To ensure the migration is successfully implemented, it is important to know what funds are available—for the initial phases of migration, for interoperability testing, and for transition to the target architecture. It is important as well to know what constraints or gaps need to be addressed. By achieving better visibility over resources, DOD can take steps needed to analyze its migration investment as well as funding alternatives.

DOD Is Developing an Architecture

DOD is in the process of developing an architecture for DCGS. It expects the architecture to be completed by July 2003. As recommended by DOD's C4ISR Architecture Framework, the architecture will include a (1) baseline, or as-is, architecture and (2) a target, or to-be, architecture. The architecture will also include a high-level concept of operations.

The architecture will to also reflect DOD's future plans to develop a web-based intelligence information network. This network would substantially change how intelligence information is collected and analyzed and could therefore substantially change DOD's requirements for DCGS. Currently, ground-surface-based systems process intelligence data and then disseminate processed data to select users. Under the new approach, unprocessed data would be posted on a Web-based network; leaving a larger range of users to decide which data they want to process and use. DOD has started implementing its plans for this new network but does not envision fully implementing it until 2010-2015.

In addition, DOD has created a DCGS Council comprised of integrated product teams to oversee the migration. A team exists for each type of

intelligence (imagery, signals, measurement, and signature); test and evaluation; and infrastructure and working groups to study specific issues.

In tandem with the architecture, DOD has also issued a capstone requirements document for the migration effort. This document references top-level requirements and standards, such as the Joint Technical Architecture with which all systems must comply. DOD is also developing an overarching test plan called the Capstone Test and Evaluation Master Plan, which will define standards, test processes, test resources, and responsibilities of the services for demonstrating that the systems can work together and an operational concept for processing intelligence information.

Planning Gaps Raise Risks

An enterprise architecture and overarching test plan should help ensure that the ground-surface-based processing systems selected for migration will be interoperable and that they will help to achieve DOD's broader goals for its intelligence operations. But there are gaps in DOD's planning that raise risks that the migration will not be adequately funded and managed.

- First, the planning process itself has been slower than DOD officials anticipated. By the time DOD expects to complete its architecture and testing plan, it will have been proceeding with its migration initiative for 4 years. This delay has hampered DOD's ability to ensure interoperability in the systems now being developed and deployed.

- Second, DOD still lacks a detailed migration plan that identifies which systems will be retained for migration; which will be phased out; when systems will be modified and integrated into the target system; how the transition will take place—how efforts will be prioritized; and how progress in implementing the migration plan and architecture will be enforced and tracked. Until DOD puts this in place, it will lack a mechanism to drive its migration. Moreover, the DCGS Council will lack a specific plan and tools for executing its oversight.

- Third, DOD has not yet developed an integrated investment strategy for its migration effort that would contemplate what resources are available for acquisitions, modifications, and interoperability testing and how gaps in those resources could be addressed. More fundamentally, DOD still lacks visibility over spending on its intelligence systems since spending is spread among the budgets of DOD's services and components. As a result, DOD does not fully know what has already

been spent on the migration effort, nor does it have a means for making sure the investments the services make in their intelligence systems support its overall goals; and if not, what other options can be employed to make sure spending is on target.

DOD officials agreed that both a migration plan and investment strategy were needed but said they were concentrating first on completing the architecture, test plan, and the operational concept.

DOD's Process for Certifying Intelligence Systems As Interoperable Is Not Working Effectively

DOD has a process in place to test and certify that systems are interoperable, but it is not working effectively for ground-surface-based intelligence processing systems. In fact, at the time of our review, only 2 of 26 DCGS systems have been certified as being interoperable. The certification process is important because it considers such things as whether systems can work with systems belonging to other military services without unacceptable workarounds or special interfaces, whether they are using standard data formats, and whether they conform to broader architectures designed to facilitate interoperability across DOD.

DOD's Process for Ensuring Interoperability

DOD has placed great importance on making intelligence processing systems interoperable and requires that all new (and many existing) systems demonstrate that they are interoperable with other systems and be certified as interoperable before they are fielded. DOD relies on the Joint Interoperability Test Command (JITC, part of the Defense Information Systems Agency) to certify systems. In conducting this certification, JITC assesses whether systems can interoperate without degrading other systems or networks or being degraded by them; the ability of systems to exchange information; the ability of systems to interoperate in joint environments without the use of unacceptable workaround procedures or special technical interfaces; and the ability of systems to interoperate while maintaining system confidentiality and integrity. In doing so, JITC reviews testing already conducted as well as assessments prepared by independent testing organizations. It may also conduct some of its own testing. The results are then submitted to the Joint Staff, who validate the system's certification. Systems are generally certified for 3 years—after which they must be re-certified.

The certification is funded by the system owner—whether it is a service or DOD agency. The cost depends on the size and complexity of a system and

generally requires 10 percent of funding designated for testing and evaluation. Generally, certification costs are small relative to the total cost of a system. The cost to certify the Army's $95 million Common Ground Station, for example, was $388,000.

To help enforce the certification process, DOD asked 4 key officials (the Under Secretary of Defense for Acquisition, Technology and Logistics; the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; the Director of Operational Test and Evaluation; and the Director, Joint Staff) in December 2000 to periodically review systems and to place those with interoperability deficiencies on a "watch list." This designation would trigger a series of progress reviews and updates by the program manager, the responsible testing organization, and JITC, until the system is taken off the list. Other DOD forums are also charged with identifying systems that need to be put on the list, including DOD's Interoperability Senior Review Panel, which is composed of senior leaders from the offices of the Under Secretary of Defense for Acquisition Technology and Logistics; the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; the Joint Staff; the Director for Programs, Analysis, and Evaluation; the Director, Operational Test and Evaluation; and U. S. Joint Forces Command.

Most Systems Are Not Certified

At the time of our review, only 2 of 26 DCGS systems had been certified by JITC. Of the remaining 24 systems; 3 were in the process of being certified; 14 had plans for certification; and 7 had no plans. (See table 1.)

Table 1: Status of DOD's Joint Interoperability Certification for Its Distributed Common Ground-Surface Systems as of December 10, 2002

System/Description	Acquisition phase	Certified[a]	In process[b]	Planned[c]	Not planned[d]	Comments
Air Force						
Deployable Shelterized System Processes and analyzes data collected by U-2	Fielded			X		Certification testing scheduled to start in fiscal year 2003.
Deployable Transit-Cased System Processes and analyzes national and tactical imagery	Fielded			X		Certification testing scheduled to start in fiscal year 2003.

(Continued From Previous Page)

System/Description	Acquisition phase	Certified[a]	In process[b]	Planned[c]	Not planned[d]	Comments
Korean Combined Operations Intelligence Center Processes and analyzes information collected by U.S. and Korean sensors	Fielded		X			Tests conducted in fiscal year 2002 and data analysis and results pending.
Ground Control Processor Processes and reports on electronic intelligence	Fielded			X		Certification testing scheduled to start in fiscal year 2003.
Deployable Ground Intercept Facility Collects, analyzes, and reports signals intelligence	Fielded			X		Certification testing scheduled to start in fiscal year 2003.
Tactical Exploitation System Intelligence Surveillance Reconnaissance Manager	Fielded			X		Test planning underway.
Navy						
Ship Signals Exploitation Equipment Allows shipboard operators to monitor and analyze signals intelligence	Fielded	X				Certification test results for the latest version of the equipment are pending.
Battle Group Passive Horizon Extension System Collects and analyzes signals intelligence	Fielded			X		Test plan complete.
Combat Direction Finding Detects, locates, and identifies signals intelligence	Fielded			X		Test plan complete.
Joint Service Imaging Processing System-Navy Receives, analyzes, and sends reports on national and tactical imagery	Fielded			X		Tests scheduled for January and February 2003.
Unmanned Aerial Vehicle Tactical Control Station Receives and transmit imagery data from unmanned aerial vehicles	Development				X	Certification program dropped due to lack of funds.
Tactical Exploitation System-Navy Receives and analyzes national and tactical electronic and imagery data	Fielded			X		The Navy is considering a JITC proposal for test support made in November 2002.

(Continued From Previous Page)

System/Description	Acquisition phase	Certified[a]	In process[b]	Planned[c]	Not planned[d]	Comments
Global Command and Control System-Maritime Integrates imagery and other intelligence data	Fielded				X	A joint interoperability certification program contained in the system's test plan, and a meeting with program manager scheduled.
Army						
All Source Analysis System Remote Workstation Processes and analyzes information from a variety of sources on the battle field	Fielded			X		Certification testing scheduled to start in fiscal year 2003.
Integrated Processing Facility Processes and analyzes signals intelligence	Fielded				X	Recently added to DCGS family of systems. No certification planned.
Home Station Operations Center Analyzes multiple types of intelligence data	Development				X	Recently added to DCGS family of systems. No certification planned.
Counterintelligence Human Intelligence Information Management System Semiautomates collection, analysis, and dissemination of human intelligence in the battle area	Fielded	X				Certified in fiscal year 2002.
Tactical Exploitation System Processes and analyzes national and tactical intelligence in the battle area	Fielded				X	Program manger told JITC in September 2002 that no further funding is available.
Guardrail Information Node Analyzes and locates electronic and communication signals	Fielded				X	No explanation provided by program manager.
Marine Corps						
Tactical Exploitation Group Receives, analyzes, and distributes tactical imagery	Fielded		X			Test conducted in October 2002, but no further testing planned in fiscal year 2003.

(Continued From Previous Page)

System/Description	Acquisition phase	Certified[a]	In process[b]	Planned[c]	Not planned[d]	Comments
Unmanned Aerial Vehicle Tactical Control System Receives and transmits imagery data from unmanned aerial vehicles	Development				X	This is the Navy-led program whose certification program was dropped due to a lack of funds.
Intelligence Analysis System Analyzes multiple types of intelligence data	Fielded			X		Test of the intelligence operating system scheduled for fiscal year 2004.
Technical Control Analysis Center Analyzes and reports national and tactical signals intelligence from several sources	Fielded			X		Test scheduled for fiscal year 2004.
Topographic Production Capability Accesses geospatial data libraries to support mapping and charting	Fielded			X		System managers not directed to begin certification program.
Tactical Electronic Reconnaissance Processing and Evaluation System Fuses signals intelligence from several sources	Fielded			X		System managers not directed to begin certification program.
Common Ground Station Receives intelligence data from the airborne joint surveillance and targeting attack radar system	Fielded		X			The Army's system has been certified and its applicability to the Marine Corps system is being assessed.

Source: DOD.

Notes: The categories provided in the table assume the following definition:

[a]*Certified*: 100 percent certification of all critical interfaces

[b]*In process*: at least 1 critical interface has been tested and/or certified

[c]*Planned*: funding is available and test planning initiated

[d]*Not planned*: No funding or agreement established for JITC testing

Because 21 systems that have not been certified have already been fielded, there is greater risk that the systems cannot share data as quickly as needed. Some of the systems in this category are critical to the success of other intelligence systems. For example, software modules contained in the Army's tactical exploitation system are to be used to build systems for the Navy, Marine Corps, and the Air Force.

DOD officials responsible for developing intelligence systems as well as testing them pointed toward several reasons for noncompliance, including the following. Our previous work in this area has identified the following similar reasons.[4]

- Some system managers are unaware of the requirement for certification.
- Some system managers do not believe that their design, although fielded, was mature enough for testing.
- Some system managers are concerned that the certification process itself would raise the need for expensive system modifications.
- DOD officials do not always budget the resources needed for interoperability testing.
- The military services sometimes allow service-unique requirements to take precedence over satisfying joint interoperability requirements.
- Various approval authorities allow some new systems to be fielded without verifying their certification status.

DOD's interoperability watch list was implemented after our 1998 report to provide better oversight over the interoperability certification process. In January 2003, after considering our findings, DOD's Interoperability Senior Review Panel evaluated DCGS's progress toward interoperability certification and added the program to the interoperability watch list.

Conclusions

Making its intelligence systems interoperable and enhancing their capability is a critical first step in DOD's effort to drive down time needed to identify and hit targets and otherwise enhance joint military operations. But DOD has been slow to plan for this initiative and it has not addressed important questions such as how and when systems will be pared down and modified as well as how the initiative will be funded. Moreover, DOD is fielding new systems and new versions of old systems without following its own certification process. If both problems are not promptly addressed,

[4] U.S. General Accounting Office, *Joint/Military Operations: Weaknesses in Department of Defense's Process for Certifying C4I Systems' Interoperability*, GAO/NSIAD 98-73 (Washington, D.C.: Mar. 1998).

data sharing problems may still persist, precluding DOD from achieving its goals for quicker intelligence dissemination. Even for the DCGS systems, which are supposed to be interconnected over time, noncompliance with interoperability requirements continues to persist. We believe DOD should take a fresh look at the reasons for noncompliance and consider what mix of controls and incentives, including innovative funding mechanisms, are needed to ensure the interoperability of DCGS systems.

Recommendations for Executive Action

To ensure that an effective Distributed Common Ground-Surface System is adequately planned and funded, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence to expand the planning efforts for DCGS to include a migration plan or road map that at a minimum lays out (1) current system capabilities and desired capabilities; (2) specific initiatives, programs, projects and schedules to get DOD and the services to their goal; (3) measures to gauge success in implementing the migration plan as well as the enterprise architecture; and (4) mechanisms for ensuring that the plan is followed.

We also recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence to develop an investment strategy to identify what funds are available, both for the initial phases of the DCGS migration and transition to the target architecture, and whether there are gaps or constraints that need to be addressed.

To ensure that systems critical to an effective DCGS are interoperable, we recommend that the Secretary of Defense take steps needed to enforce its certification process, including directing the service secretaries in collaboration with the Joint Staff, Acquisition Executives, and the Joint Interoperability Test Command to (1) examine reasons the services are slow to comply with its certification requirement and (2) mechanisms that can be implemented to instill better discipline in adhering to the certification requirement. If lack of funding is found to be a significant barrier, we recommend that the Secretary of Defense consider centrally funding the DCGS certification process as a pilot program.

Agency Comments and Our Evaluation

In commenting on a draft of this report, DOD concurred with our recommendations to expand the planning efforts for DCGS to include a migration plan and an investment strategy. It stated that it has already funded both projects. DOD also strongly supported our recommendation to take additional steps to enforce its certification process and described recent actions it has taken to do so. DOD partially concurred with our last recommendation to consider centrally funding the certification process if funding is found to be a significant barrier. While DOD supported this step if it is warranted, DOD believed it was premature to identify a solution without further definition of the problem. We agree that DOD needs to first examine the reasons for noncompliance and consider what mix of controls and incentives are needed to make the certification process work. At the same time, because funding has already been raised as a barrier, DOD should include an analysis of innovative funding mechanisms into its review.

Scope and Methodology

To achieve our objectives, we examined Department of Defense regulations, directives, instructions as well as the implementing instructions of the Chairman, Joint Chiefs of Staff, regarding interoperability and the certification process. We visited the Joint Interoperability Test Command in Fort Huachuca, Arizona, and obtained detailed briefings on the extent that intelligence, surveillance, and reconnaissance systems, including DCGS systems, have been certified. We visited and obtained detailed briefings on the interoperability issues facing the Combatant Commanders at Joint Forces Command in Norfolk, Virginia; Central Command in Tampa, Florida; and Pacific Command in Honolulu, Hawaii, including a videoconference with U.S. Forces Korea officials. We discussed the interoperability certification process and its implementation with officials in the Office of the Director, Operational Test and Evaluation; the Under Secretary of Defense for Acquisition, Technology and Logistics; and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. During these visits and additional visits to the intelligence and acquisition offices of the services, the National Imagery and Mapping Agency, and the National Security Agency, we obtained detailed briefings and examined documents such as the capstone requirements document involving the status and plan to implement the ground systems strategy. We conducted our review from December 2001 through February 2003 in accordance with generally accepted government auditing standards.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 7 days from the date of this report. At that time, we will send copies of this report to the other congressional defense committees and the Secretary of Defense. We will also provide copies to others on request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

Please contact me at (202) 512-4841 if you or your staff have any questions concerning this report. Key contributors to this report were Keith Rhodes, Cristina Chaplain, Richard Strittmatter, and Matthew Mongin.

R.E. Levin
Director, Acquisition and Sourcing Management

Comments from the Department of Defense

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

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

Mr. Robert E. Levin
Director, Acquisition and Sourcing Management
U.S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Levin:

This is the Department of Defense (DoD) response to the GAO draft report, "DEFENSE ACQUISITIONS: Steps Needed To Ensure Interoperability of Systems That Process Intelligence Data" dated February 10, 2003, (GAO Code 120115/GAO-03-329).

This response has been prepared by OASD (C3I)/ISR Programs as the Primary Action Office after reviewing comments from the Collateral Action Offices. The Department accepts and CONCURS with Recommendations 1, 2, and 3 and PARTIALLY CONCURS with Recommendation 4. Responses to each recommendation are provided on the attached comment sheets.

In addition to responses to GAO recommendations, you will find a fifth attachment that suggests changes to the body of the report in areas that the Department feels are in error or require additional information.

We appreciate the opportunity to provide this information and look forward to further dialogue on this matter.

Sincerely,

for Kevin P. Meiners
Director, OASD (C3I)/ISR Programs

Attachments:
Comment Sheets (4)
Suggested Change Matrix

GAO DRAFT REPORT – DATED FEBRUARY 10, 2003
GAO CODE 120115/GAO-03-329

"DEFENSE ACQUISITIONS: STEPS NEEDED TO ENSURE INTEROPERABILITY OF SYSTEMS THAT PROCESS INTELLIGENCE DATA"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1:

The GAO recommended that the Secretary of Defense direct the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to expand the planning efforts for Distributed Common Ground/surface Systems (DCGS) to include a migration plan or roadmap that, at a minimum, lays out: (1) current system capabilities and desired capabilities, (2) specific initiatives, programs, projects and schedules, to get DoD and the Services to their goal, (3) measures to gauge success in implementing the migration plan as well as the enterprise architecture, and (4) mechanisms for ensuring that the plan is followed. (p. 18/GAO Draft Report)

DoD RESPONSE: CONCUR

DoD COMMENTS:

A roadmap development effort has been identified as the objective activity for the DoD's Architecture Development effort discussed on pages 9 and 10 of the GAO report. The sequence of events of an operational concept definition, architectural product creation, and shortfalls analysis all lead to the generation of a roadmap that will contain necessary policy, programmatic, and resource decision points and migration paths. The roadmap activity is funded in FY 03 and is to begin shortly.

GAO DRAFT REPORT – DATED FEBRUARY 10, 2003
GAO CODE 120115/GAO-03-329

"DEFENSE ACQUISITIONS: STEPS NEEDED TO ENSURE INTEROPERABILITY OF SYSTEMS THAT PROCESS INTELLIGENCE DATA"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 2:

The GAO recommended that the Secretary of Defense direct the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) to develop an investment strategy to identify what funds are available, both for the initial phases of the DCGS migration and transition to the target architecture, and whether there are gaps or constraints that need to be addresses. (p. 18 GAO Draft Report)

DoD RESPONSE: CONCUR

DoD COMMENTS:

As part of the roadmap activity planned for FY 03, the necessary investments will be captured as part of the resource decision points outlined in that roadmap.

GAO DRAFT REPORT – DATED FEBRUARY 10, 2003
GAO CODE 120115/GAO-03-329

"DEFENSE ACQUISITIONS: STEPS NEEDED TO ENSURE INTEROPERABILITY OF SYSTEMS THAT PROCESS INTELLIGENCE DATA"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 3:

The GAO recommended that the Secretary of Defense take steps needed to enforce its certification process, including directing the Service Secretaries in collaboration with the Commander, Joint Interoperability Test Command, to; (1) examine reasons the Services are slow to comply with its certification requirement, and (2) examine mechanisms that can be implemented to instill better discipline in adhering to the certification requirement. (p. 18/GAO Draft Report)

DoD RESPONSE: CONCUR

DoD COMMENTS:

The Department strongly supports this recommendation. This is evidenced by recent activities to improve interoperability enforcement including publication of DODD 4630.5 and DODI 4630.8, the Interoperability Senior Review Panel (ISRP) review of DCGS, the DCGS Capstone Test & Evaluation Master Plan (CTEMP), and the development of DCGS Compliance Level criteria that will support Joint Interoperability Certification.

Successful implementation of the recommended steps will require the Joint Staff, who promulgates CJCSI 6212.01B and validates system JICs from JITC, and the Service Acquisition Authorities that are key to effective implementation by their System Program Managers, to participate in the process.

The additional actions suggested under this recommendation are areas that must be incorporated into the DCGS program to ensure migration and transformation to the defined objective state captured in the DCGS Capstone Requirements Document (CRD) and the DCGS architectural products. All of these considerations and issues will be addressed in the DoD DCGS roadmap activity. It will address not only materiel but also policy and other non-materiel solutions.

GAO DRAFT REPORT – DATED FEBRUARY 10, 2003
GAO CODE 120115/GAO-03-329

"DEFENSE ACQUISITIONS: STEPS NEEDED TO ENSURE INTEROPERABILITY OF SYSTEMS THAT PROCESS INTELLIGENCE DATA"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 4:

The GAO recommended that, if lack of funding is found to be a significant barrier, the Secretary of Defense consider centrally funding the DCGS certification process as a pilot program. (p. 18 GAO Draft Report)

DoD RESPONSE: PARTIALLY CONCUR

DoD COMMENTS:

While the GAO recommends centrally funding the DCGS certification process as a pilot program if lack of funding is found to be a significant barrier, the Department believes it is premature to identify a solution without further definition of the problem. The Department identified this problem and placed DCGS on the Interoperability Watch List. This will result in increased emphasis. If this proves to be insufficient, then a centrally funded effort may be warranted.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to GAO Mailing Lists" under "Order GAO Products" heading.

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. General Accounting 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

Public Affairs

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

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

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00