



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

March 1998

JOINT MILITARY OPERATIONS

Weaknesses in DOD's Process for Certifying C4I Systems' Interoperability



CONFIDENTIAL - SECURITY INFORMATION
Approved for public release
Distribution unlimited

19980317 123

National Security and
International Affairs Division

B-279021

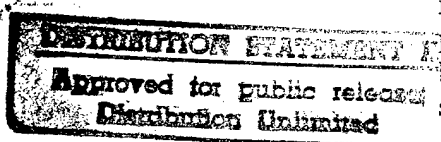
March 13, 1998

DTIC QUALITY INSPECTED 2

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

Dear Mr. Chairman:

Command, control, communications, computers, and intelligence (C4I) systems relay critical information to U.S. forces during joint operations. If joint operations are to be successful, C4I systems must be “interoperable”—capable of exchanging information and operating effectively together. To help ensure interoperability, the Defense Information Systems Agency (DISA)—under the direction of the Joint Chiefs of Staff—established the current certification process in 1992. According to Joint Staff guidance, commanders in chief, the four services, and Department of Defense (DOD) agencies are required to use this process to test and certify existing and newly developed systems for interoperability. Generally, newly developed systems are to be denied production approval if they have not been certified. After a system has been fielded and a modification is made that affects interoperability, the system must be recertified.



In response to your request, we determined (1) whether DOD organizations are complying with interoperability testing and certification requirements and (2) what actions, if any, are needed to improve the current certification process. We also identified initiatives that affect interoperability; they are discussed in appendix I.

Background

The military services have a long history of interoperability problems during joint operations. For example, the success of the Persian Gulf war in 1991—a major joint military operation—was hampered by a lack of basic interoperability. The current certification requirement was established to help address these problems. The Joint Staff's Director for C4 systems (J-6) is assigned primary responsibility for ensuring compliance with the certification requirement. DISA's Joint Interoperability Test Command is the sole certifier of C4I systems. According to Joint Staff guidance, commanders in chief, the services, and DOD agencies are required to adequately budget for certification testing. They can either administer their own tests with Test Command oversight or ask the Test

Command to administer them. Certification is intended to help provide the warfighter with C4I systems that are interoperable and to enable forces to exchange information effectively during a joint mission. Specifically, certification by the Test Command is confirmation that (1) a C4I system has undergone appropriate testing, (2) the applicable requirements for interoperability have been met, and (3) the system is ready for joint use. However, while a system may pass certification testing, it may not have been tested against all systems with which it may eventually interoperate. This is because some systems with which they must interoperate become available later and commanders sometimes use systems in new ways that were not envisioned during testing.

DOD guidance requires that a system be tested and certified before approval to produce and field it. Depending on the acquisition category and dollar threshold of the program,¹ the approval authority may be the Under Secretary of Defense (Acquisition and Technology), with advice from the Defense Acquisition Board; the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), with advice from the Major Automated Information System Review Council; or the DOD component head (such as the commander in chief of a unified combatant command, the head of a military service, or a DOD agency head).

A DOD Directive established the Military Communications Electronics Board to provide guidance on interoperability issues referred to it by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff. The Board addresses interoperability issues through two subpanels: (1) The Interoperability Improvement Panel monitors C4I interoperability issues surfaced by the commanders in chiefs, military services, and DOD agencies and (2) The Interoperability Test Panel resolves testing disputes (such as appeals of Test Command certification decisions made by commanders in chief, military services, and DOD agencies). The Test Panel may waive the certification requirement to support developmental efforts, demonstrations, exercises, or normal operations. The waiver is not intended to be permanent, and is typically granted for 1 year.

Results in Brief

DOD does not have an effective process for certifying existing, newly developed, and modified C4I systems for interoperability. As a result, many C4I systems have not been certified for interoperability and, in fact, DOD does not know how many require certification. Improvements to the

¹DOD has four traditional acquisition categories—major defense programs, major automated system programs, other major programs, and nonmajor acquisition programs.

certification process are needed to provide DOD better assurance that C4I systems critical to effective joint operations are tested and certified for interoperability.

DOD organizations are not complying with the current interoperability testing and certification process for existing, newly developed, and modified C4I systems. According to Test Command officials, many C4I systems that require interoperability testing have not been certified or have not received a waiver from the requirement. The extent of this noncompliance could have far-reaching effects on the use of such systems in joint operations. For example, a modified C4I system that was not recertified experienced an interoperability problem exchanging data with another system. The result was the simulated downing of a commercial airplane during a joint exercise.

Noncompliance with interoperability testing and certification stems from weaknesses in the certification process itself. While DOD guidance requires that all new systems be certified or obtain a waiver from certification testing before they enter production and fielding, systems proceed to these latter acquisition stages without being certified. This occurs, in part, because Test Command officials lack the authority to compel DOD organizations to submit their C4I systems for testing. Although DOD guidance spells out a specific interoperability certification requirement, many DOD organizations are unaware of it. Others simply ignore the requirement because it is not strictly enforced or because they do not adequately budget for such testing.

Another fundamental weakness in the process is the lack of a complete and accurate listing of C4I systems requiring certification and a plan to prioritize systems for testing. As a result, the Test Command may not be focusing its limited resources on certifying the most critical systems first. Prioritization is important since the Command has reviewed only about 100 systems per year, and a requirement for recertification of modified systems continually adds to the number of systems requiring certification. The process also does not include a mechanism to notify the services about interoperability problems identified in joint exercises, and the Test Command has only recently begun to contact the services regarding the noted problems. Finally, the Test Panel does not have a formal process to inform DOD organizations that systems with expired waivers require an extension or certification. Accordingly, six of nine systems with expired waivers have not had the waiver extended or been tested and certified.

Compliance With Certification Requirement Is Inadequate

Commanders in chief, services, and DOD agencies are generally not complying with the certification requirement. As a result, we found instances in which existing, newly fielded, and modified systems are not certified for interoperability. Test Command analysis showed that a significant number of existing C4I systems had not been submitted for certification as required. According to Test Command officials, as of December 1997, the DOD Defense Integration Support Tool database of C4 systems listed about 1,000 systems that may exchange information with another system. In addition, there are about 1,176 unclassified intelligence systems, according to the Office of the Assistant Secretary of Defense, C3I. Test Command officials said they did not know precisely how many of these systems require certification. Nor did the Office of the Assistant Secretary of Defense know which intelligence systems would require certification because they were unable to determine which of these systems were outdated (i.e., legacy systems), stand alone systems, or one-service-only systems. While the Test Command has generally certified increasingly more systems during the past 4 years, officials acknowledged that "they have not even begun to scratch the surface" of the universe of systems that may require testing and certification. During fiscal years 1994 through 1997, the Test Command certified 149 C4I systems.

According to Test Command officials, DOD's Defense Integration Support Tool database attempts to list all C4 systems and other mission critical systems, but it does not contain all C4 systems or indicate whether the systems have been certified. According to DISA documentation, the purpose of the Defense Integration Support Tool is to support a DOD-wide information management requirement for data collection, reporting, and decision support in areas such as planning and interoperability. After discussions with DOD officials regarding this issue, DOD has recently included certification status as part of the database and, as of January 1998, 44 systems reflected this information.

We recently reported in two separate reports that the Defense Integration Support Tool database is incomplete and inaccurate.² In response to our October 1997 report, DOD acknowledged that this database is its official automated repository and backbone management tool for DOD's inventory of systems. Accordingly, DOD said that it had begun to take major actions to enhance the database by instituting a validation and data quality program to ensure that the database contains accurate and complete data. DOD further stated that it would closely monitor this program to ensure

²Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, Aug. 13, 1997) and Defense IRM: Poor Implementation of Management Controls Has Put Migration Strategy at Risk (GAO/AIMD-98-5, Oct. 20, 1997).

that the data quality is at the highest level as required for reports to senior Defense managers and the Congress. Since this database is an important management tool, it is essential that it be complete and accurate.

In several instances, new systems have been fielded without consideration of the certification requirement. Two recently fielded Air Force systems—a weather prediction system and a radar system—were not tested for certification by the Test Command, despite June 1996 memorandums from the Joint Staff stating that the service must plan for testing to ensure compliance with interoperability guidelines. Further, since 1994, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) has approved three of nine major automated information systems for production and fielding that had not been certified for interoperability. For example, the recently fielded Defense Message System was not certified by the Test Command. Test Command officials stated that the system has undergone some interoperability testing but, because of shortfalls, was not certified. A decision was made to field the system while the shortfalls are resolved. Test Command officials believe the system will eventually be certified.

No newly developed systems purchased through the Command and Control Initiatives Program were tested by the Test Command. (This program allows commanders in chief to purchase low-cost improvements to their command and control systems.) According to DISA officials, DISA had assessed these systems' interoperability requirements and reminded the users to submit the systems for testing. In addition, during the last 3 years, no systems purchased through the Advanced Concept Technology Demonstrators program were tested and certified. (This program allows a new capability to be quickly developed, purchased, and exercised in the field before an acquisition commitment is made.)

According to Test Command officials, previously certified systems that were later modified are not consistently submitted for recertification as required. Although Test Command officials do not know the exact number of modified systems that require recertification, they are aware of several systems—such as the Navy's AEGIS shipboard weapon system and the Air Force's Airborne Warning and Control System.

Reasons for Inadequate Compliance

Joint Staff officials believe that, although the certification requirement is outlined in several DOD and Joint Staff guidance documents, some system managers are unaware of it.³ In a study chartered by J-6 and completed in January 1996, only 12 of 424 (less than 3 percent) surveyed acquisition managers and Defense System Management College students knew about the DOD and Joint Staff interoperability requirements. The study team found that this lack of knowledge prevented users from placing interoperability in the initial requirements documents and acquisition managers from building interoperability into approved programs. As a result, the Joint Staff began an effort in 1996 to better educate system managers about the requirement. However, the study points out that education is not a panacea for all interoperability problems.

Our analysis showed that some DOD organizations, although aware of the requirement, did not submit fielded systems for testing. For example, some program managers did not submit their modified systems for certification because they believed their design, although fielded, was not mature enough for testing. The program managers did not seek a waiver for their systems and ignored the certification requirement. Test Command officials told us that they lack the authority to compel program managers to bring their systems in for testing and must rely on the managers' cooperation.

In addition, in fiscal year 1995, only three intelligence systems were certified by the Test Command. Because Test Command officials believed that DOD's intelligence community was ignoring the certification requirement, in 1996 the Command negotiated an agreement with DOD's Intelligence Information Systems Management Board (which has responsibility for a portion of intelligence systems) to facilitate better participation in the certification process. In fiscal year 1997, the number of intelligence systems tested and certified increased to 14. Test Command officials believe that the increase is a direct result of the agreement.

Further, according to Test Command officials, DOD officials do not always budget the resources needed for interoperability testing as required by Joint Staff guidance. In certain cases, the services do not budget sufficient funds to cover secondary C4I systems that are used to test the primary C4I system for interoperability because the services cannot afford to pay for all the testing DOD policy requires. For example, the services are required to provide secondary systems for 10 tactical data link interoperability tests

³The primary DOD interoperability guidance documents are DOD Directive 4630.5, November 12, 1992; DOD Instruction 4630.8, November 18, 1992; and Chairman of the Joint Chiefs of Staff Instruction 6212.01A, June 30, 1995.

a year. In this case, however, according to a Test Command official, the Army budgets for only seven or eight tests a year. The services are responsible for acquiring systems that satisfy service-unique requirements, and this responsibility sometimes takes precedence over satisfying joint interoperability requirements. In his 1996 report to the Secretary of Defense, the Chairman of the Joint Chiefs of Staff recommended that funding for DOD C4I systems be reviewed, since the services' funding decisions may not further DOD's overall goal of promoting C4I joint interoperability.

Finally, the various approval authorities are allowing some new systems to be fielded without verifying their certification status. According to a Joint Staff J-6 spokesman, the Joint Staff J-6 representative is to ensure that interoperability certification is addressed at the approval authority acquisition meetings. If the Joint Staff J-6 representative is unable to attend these meetings, the issue of certification is not raised. However, J-6 coordination is obtained on all acquisition decision memorandums granting production and fielding approval. Nevertheless, systems receive approval for production and fielding even though they may not have been certified or obtained waivers.

Examples of Interoperability Problems That Are Not Being Addressed

In several instances, the Test Command identified interoperability problems in systems that DOD organizations had not submitted for testing. The following are examples:

In 1996, the Test Command expressed concerns to the Air Force that its Joint Tactical Information Distribution System, a computer terminal used to provide surveillance data on F-15 aircraft, had not been certified. The system (a proof of concept demonstration) had operated for 3 years. According to a Test Command memorandum, Command representatives witnessed numerous interoperability problems caused by this system during joint exercises. The memorandum indicated that if the exercise had been a real world situation, the system's interoperability problems could have resulted in numerous deaths of pilots and enemy penetrations of U.S. airspace. In a written response, the Air Force stated that it disagreed with the Test Command's assessment of the problems. Furthermore, the Air Force said that certification of the system was not the best use of resources because the Air Force planned to eventually replace it. According to Test Command officials, the system is scheduled for testing in 1998. Still not certified, the system has been operational for over 1 year since the Air Force's response.

Test Command officials have been unable to persuade the Navy's AEGIS program office to submit all fielded versions of the ship's weapon system for interoperability testing. Command representatives have observed the weapon system experiencing significant interoperability problems in several recent joint exercises. The Test Command is aware of five fielded versions of AEGIS software, and the program office states there are many more. However, the Test Command has tested and certified only the oldest version (in May 1995), the most basic of the five versions. The need for interoperability certification testing of the uncertified versions has been discussed at joint interoperability meetings and with DISA. The responsible DISA official requested, under Test Command letterhead, that AEGIS submit uncertified versions for joint testing. However, according to AEGIS program officials, none of these versions has been jointly tested because the newer versions either have not yet been tested with other Navy-only systems or are not yet demonstrating adequate interoperability performance in testing with Navy-only systems.

The Test Command has been unable to persuade users to test DOD's Air Defense System Integrator, which provides tactical data link translation and message-forwarding functions. The system has been acquired outside the normal DOD acquisition process. About 30 versions of this system have been fielded; none has been jointly tested. According to Test Command officials, the system is experiencing significant interoperability problems because it does not conform to required standards. Interoperability problems with this system could result in hostile systems leaking through U.S. defenses or friendly systems being attacked. Without certification of the interfaces that translate and forward messages among systems, for example, the proper tracking and targeting information may not be provided to our theater air missile defense system. At several 1997 meetings with representatives from all the services, the Joint Staff, and the Test Command, problems with the system were discussed. Solutions are still being developed and implemented.

Weaknesses Exist in DOD's Certification Process

Noncompliance with interoperability testing and certification stems from weaknesses in the certification process itself. For example, DOD lacks a complete and accurate listing of C4I systems requiring certification and a plan to prioritize systems for testing. As a result, the Test Command may not be focusing its limited resources on certifying the most critical systems first. The process also does not include a mechanism to notify the services about interoperability problems identified in joint exercises, and the Test Command has only recently begun to contact the services

regarding the noted problems. Finally, according to a Test Panel official, the Panel does not have a formal process to inform DOD organizations that systems with expired waivers require an extension or certification.

DOD Lacks a Plan to Prioritize Testing and Has Not Identified Critical Systems to Be Certified

Neither the Joint Staff nor DISA has given the Test Command a priority list for testing C4I systems. As a result, the Command tests systems without regard to systems that should receive a high priority for testing. Test Command officials believe that such a list would help them better plan their test schedule. Generally, the Command develops a master test schedule based on the notification of systems ready for testing by the commanders in chiefs, services, and DOD agencies. As these notifications are received, the Command updates its schedule.

Furthermore, DOD has not identified the exact number of systems to be certified. A Command official told us that, even if systems are identified, it is difficult to test all C4I systems required to be certified. According to Test Command officials, they are able to test no more than 200 systems per year. Our analysis shows that the Command generally reviews about 100 systems per year and in 1997 certified 44 individual systems for interoperability (not including systems receiving multiple certifications due to modifications or testing with additional systems). According to the official, a list prioritizing systems for testing would assist the Command to use its scarce resources to test the most important systems first.

In June 1996, the Military Communications Electronic Board reviewed existing command and control systems submitted by the services and determined that 42 were crucial to the needs of military commanders. Our analysis showed that, as of October 1997, 23 had not been tested or certified. According to Test Command officials, the 23 systems were not certified for various reasons. The officials stated that they did not know about 13 of the systems; 7 are scheduled or are to be scheduled for testing, but the schedules could slip; 2 were not submitted for testing by the commanders in chief, service, or DOD agency because 1 is a low priority for testing and the other needs redesign (although both have been operational for several years); and 1 was considered too immature to test. Without an approved DOD-wide testing strategy, the Test Command's scarce resources may not be best used to test the right C4I systems at the right time.

Joint Staff, Test Command, and commander in chief officials believe that one area that should receive high priority in any plan for interoperability testing is theater air and missile defense systems. This functional area is

heavily dependent on systems being interoperable. According to Test Command officials, about 100 major systems are involved in theater air and missile defense, and about 45 percent of these have not been tested or certified for interoperability. DOD officials stated that significant interoperability problems in these defense systems could have dire consequences for joint and coalition forces. Some joint exercises conducted during the last 2 years have demonstrated the need for better interoperability in this functional area. Interoperability problems in these exercises resulted in the simulated downing of friendly aircraft in one exercise and in the nonengagement of hostile systems in another.

Test Command Does Not Advise the Services About Interoperability Problems

Test Command officials stated that they do not generally advise services' system program managers on interoperability problems identified in exercises. While not required to do so, the Test Command is in the best position to advise the commanders in chief, services, and DOD agencies because according to Command officials they discover, evaluate, and document these problems. As part of its mission and apart from certification testing, the Command provides operational support and technical assistance to the commanders in chief, the services, and DOD agencies during exercises.

In reports summarizing the results of four joint exercises during 1996 and 1997, the Test Command noted that 15 systems experienced 43 "significant interoperability problems"—defects that could result in the loss of life, equipment, or supplies. The vast majority of these problems were caused by system-specific software problems. Specific problems experienced included

- failure to accept changes in mislabeled data identifying a friendly aircraft as a hostile aircraft, thereby causing the simulated downing of a commercial airliner;
- excess messages overloading systems, causing system crashes and the loss of command and control resources during critical periods;
- improper track identification, creating the potential for either a hostile system to penetrate defenses or a friendly system to be inadvertently destroyed; and
- duplicate tracks distorting the joint tactical picture, denying vital information to battle managers and shooters.

In table 1, we list the 15 systems that experienced significant problems and indicate their certification status.

Table 1: Certification Status of C4 Systems Experiencing Significant Interoperability Problems in Four Joint Exercises During 1996 and 1997

C4 system	Number of significant interoperability problems	Certification status		
		Certified ^a	Uncertified	Modified but not recertified
PATRIOT	8	X		
AEGIS	7			X
Shelterized Joint Tactical Information Distribution System	6		X	
Modular Control Equipment	4	X		
Airborne Warning and Control System	3			X
Airborne Surveillance Testbed	3		X	
Tactical Air Operations Module	2	X		
Joint Tactical Ground Station	2		X	
Air Defense System Integrator	2		X	
EP-3E ARIES aircraft	1		X	
F-15 aircraft	1		X	
F-14 aircraft	1		X	
Airborne Laser ^b	1		X	
Theater High-Altitude Air Defense ^c	1		X	
Expert Missile Tracker	1		X	
Total	43			

^aEven though a system is certified, significant problems not identified during testing can arise in an exercise due to the less-controlled environment. Also, systems used in exercises often are linked by radio rather than direct cable connection, introducing the potential for missing information. Other problems with certified systems could surface because new systems with which they must interoperate might not have been in the force when testing occurred. Also, commanders sometimes use systems in ways not envisioned during testing.

^bThis system has not yet been approved for production and fielding and has not been tested for interoperability by the Test Command.

^cSome components of this system participated in a joint exercise. Interoperability testing is scheduled to begin in March 1999.

Source: Our analysis of 1996 and 1997 Joint Interoperability Test Command exercise reports.

When the services' program managers are not advised, significant interoperability problems may arise in subsequent exercises and operations. According to Test Command officials, after our inquiries the Command began exploring ways to formally track and follow up on these problems. After our visit, Command officials stated they were beginning to identify the problem systems and contact the program managers to request

that systems be retested. However, as of December 1997, Command officials had contacted only three system managers, and none of the systems have been tested.

Test Panel Does Not Have a Formal Process for Informing DOD Organizations About Expired Waivers

According to a Test Panel official, the Panel does not have a formal process to ensure that fielded systems with expired waivers are tested. As a result, most systems with expired waivers were allowed to operate without testing or an extension of the waiver. According to Panel documents, 13 waivers have been granted since May 1994. Of the 13 waivers granted, 3 have not expired and 1 was recently extended after the original waiver had been expired for 4 months (even though the system has caused interoperability problems). The remaining nine waivers have expired. Of these nine, only three are for systems that have had some interoperability testing and certification by the Test Command. Of the remaining six systems with expired waivers, two were expired for less than a year, two were expired for more than a year, and two were expired for more than 2 years.

Conclusions

Commanders in chief, the services, and DOD agencies are generally not complying with the C4I certification requirement. Inadequate compliance with this requirement increases the likelihood that C4I systems will not be interoperable, thereby putting lives, expensive equipment, and the success of joint military operations at greater risk. Improvements to the certification process are needed to provide better assurance that C4I systems most critical to joint operations are certified for interoperability. Better information is needed to track the status of waivers. Finally, the risks associated with operating uncertified systems in joint operations is heightened when systems are permitted to proceed into production and fielding without full consideration of the certification requirement.

Recommendations

To ensure that systems critical to effective joint operations do not proceed to production without due consideration given to the need for interoperability certification, we recommend that the Secretary of Defense require the acquisition authorities to adhere to the requirement that C4I systems be tested and certified for interoperability prior to the production and fielding decision unless an official waiver has been granted.

To improve the process for certifying C4I systems for interoperability, we recommend that the Secretary of Defense, in consultation with the Chairman of the Joint Chiefs of Staff, direct the

- service secretaries, in collaboration with the Director of DISA to verify and validate all C4 data in the Defense Integration Support Tool and develop a complete and accurate list of C4I systems requiring certification and
- Director of DISA to ensure that the status of system's certification is added to the Defense Integration Support Tool and that this database be properly maintained to better monitor C4 systems for interoperability compliance.

We also recommend that the Secretary of Defense request that the Chairman of the Joint Chiefs of Staff direct the

- Joint Staff (in collaboration with the commanders in chief, the services, and the Director of DISA) to develop a process for prioritizing C4I systems for testing and certification and
- Joint Staff (in collaboration with the commanders in chief, the services, and the Director of DISA) to develop a formal process to follow up on interoperability problems observed during exercises, report the problems to the relevant DOD organization, and inform organizations that the systems are required to be tested for interoperability.

We recommend that, to improve DOD's information on the status of waivers from interoperability certification, the Chairman of the Joint Chiefs of Staff establish a system to monitor waivers. The system should inform DOD organizations when waivers expire and request that they either seek an extension of the waivers or test their systems for interoperability.

Agency Comments

In written comments on a draft of this report, DOD generally concurred with all of our recommendations noting that a number of efforts are underway to improve the interoperability certification process. To improve the process, DOD is revising relevant policy and procedures to enhance their adequacy (in terms of clarity, enforcement, and integration of effort) and is improving the accuracy and utility of its Defense Integration Support Tool database. Agreeing with the need to prioritize systems for testing, DOD stated it will develop a process to set priorities for testing and certification. To follow up on interoperability issues learned during exercises, DOD intends to use several sources of information to develop a formal process to ensure identified problems are adequately addressed by the appropriate organizations. DOD also intends to revise the

charter of the Test Panel to require quarterly review of waivers from certification testing. DOD's comments are reprinted in appendix II. DOD also provided technical comments, which we have incorporated where appropriate.

Scope and Methodology

To determine whether DOD organizations were complying with the certification requirement, we analyzed DOD data on C4I systems to identify systems' certification status. Specifically, we obtained a listing of all C4 systems in the Defense Integration Support Tool from DISA Headquarters in Arlington, Virginia, and the number of unclassified intelligence systems from the Office of the Assistant Secretary of Defense, C3I in Arlington, Virginia. We compared the systems on these lists with a list of all systems certified from October 1993 through September 1997 obtained from the Joint Interoperability Test Command in Fort Huachuca, Arizona. We also obtained a list of C4I systems included in Command and Control Initiatives Program budget proposals from October 1994 through September 1997 and a listing of C4I systems included in DOD's Advanced Concept Technology Demonstrators program. We compared these lists with the Test Command's list of certified systems. We did not verify the accuracy or validity of any DOD list.

We also obtained, reviewed, and analyzed DOD policy, Joint Staff instructions, and other documents regarding compatibility, interoperability, and integration of C4I systems. We obtained these documents and discussed interoperability issues in the Washington, D.C., area in interviews with cognizant officials from the Office of the Deputy Under Secretary of Defense (Advanced Technology); the Office of the Assistant Secretary of Defense, C3I; the Office of the Director, Operational Test and Evaluation; the Joint Chiefs of Staff Directorate for C4 (J-6); the Directorate for Force Structure, Resources and Assessment (J-8); and DISA. In addition, we reviewed documents and interviewed cognizant officials regarding interoperability issues, including certification of C4I systems, from the U.S. Atlantic Command, Norfolk, Virginia; U.S. Central Command, MacDill Air Force Base, Florida; U.S. Pacific Command, Camp Smith, Hawaii; U.S. European Command, Germany; the Naval Center for Tactical Systems Interoperability, San Diego, California; U. S. Army Communications and Electronics Command, Fort Monmouth, New Jersey; and individual system program offices or support activities in each of the military services, including the Navy AEGIS program office, Dahlgren, Virginia; the Air Force Air Combat Command Directorate of Operations for Command and Control and Intelligence, Surveillance, and

Reconnaissance, Langley Air Force Base, Virginia; the Army Communications and Electronics Command Software Engineering Center, Fort Monmouth, New Jersey; and the Naval Air Warfare Center, Weapons Division, Point Mugu, California.

To determine whether improvements were needed in the certification process, we interviewed Test Command officials on interoperability and certification issues, including testing priorities and exercise problem follow-up, and compared the Command's list of certified systems from October 1993 through September 1997 with a June 14, 1996, list of DOD's crucial C2 systems. We also reviewed reports on lessons learned and demonstrations and exercises obtained from the Joint Staff J-8 and the Test Command, respectively, to identify C4I systems with interoperability problems. We then compared the problem C4I systems with the Test Command's certification list to analyze whether the systems were certified, uncertified, or modified and not recertified. We also interviewed officials and obtained and analyzed waiver documents from the Military Communications Electronics Board's Interoperability Test Panel. We reviewed the waivers to determine the reasons for them and the time period involved.

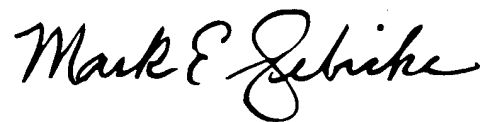
Finally, to determine initiatives that affect interoperability, we reviewed DOD's C4I for the Warrior concept; the Defense Information Infrastructure Master Plan; the 1996 assessment of combat support agencies report by the Chairman of the Joint Chiefs of Staff; the 1996 Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance Task Force reports; and the Levels of Information System Interoperability reports by the Task Force.

We conducted our review from January 1997 to January 1998 in accordance with generally accepted government auditing standards.

We are sending copies of this report to the Secretaries of Defense, the Army, the Navy, and the Air Force and other appropriate congressional committees. Copies will also be made available to others on request.

Please contact me at (202) 512-5140 if you or your staff have any questions concerning this report. Major contributors to this report are listed in appendix III.

Sincerely yours,



Mark E. Gebicke
Director, Military Operations
and Capabilities Issues

Contents

Letter	1
Appendix I DOD Initiatives to Improve the Interoperability of C4I Systems	20
Appendix II Comments From the Department of Defense	23
Appendix III Major Contributors to This Report	28
Table	11

Table 1: Certification Status of C4 Systems Experiencing Significant Interoperability Problems in Four Joint Exercises During 1996 and 1997

Abbreviations

C4I	command, control, communications, computers, and intelligence
DISA	Defense Information Systems Agency
DOD	Department of Defense

DOD Initiatives to Improve the Interoperability of C4I Systems

Improving ways of complying with the certification process alone will not solve all of the issues related to interoperability. The Department of Defense (DOD) has a number of initiatives underway that address various aspects of interoperability: the C4I for the warrior concept; the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Architecture Framework; the Defense Information Infrastructure strategy; and the Levels of Information Systems Interoperability initiative.

Initiated in 1992, the C4I for the warrior concept is to provide a global command, control, communications, computer, and intelligence system that directly links and supports the combat troops of all services who engage in military operations. The system will display anywhere around the world a real-time, true picture of the battlespace, detailed mission objectives, and a clear view of enemy targets. This advanced technology concept is to support DOD's vision for the evolution of the U.S. armed force's capabilities to the year 2010.

The Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Architecture Framework, published in June 1996 by the DOD Integration Task Force, is to address a DOD-wide lack of a shared understanding of the architecture process and insufficiently precise terminology. According to the Task Force, architectures can be a key factor in guiding and controlling the acquisition and evolution of interoperable and efficient C4I systems. If adopted, the framework will provide a common approach for the commanders in chief, the services, and DOD agencies to follow in developing their C4I architectures. The Task Force report stated that the framework has, in part, the ultimate potential of "facilitating, improving, and ensuring compatibility, interoperability, and integration among command, control, communications, computers, intelligence, surveillance, and reconnaissance capabilities." While a final report was issued in June 1996, the framework has not been implemented as DOD policy. Currently, adoption of the framework in DOD policy is not planned according to a Joint Staff official. A current version of the framework itself was issued in July 1998. However, a J-6 official expects full implementation to take 1 to 2 years after its publication.

DOD issued a Defense Information Infrastructure master plan in November 1994 to integrate its communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet DOD's information processing and

transport needs. The plan is updated periodically and provides a description of the Defense Information Infrastructure's major components.

The infrastructure is largely an unintegrated collection of systems with unique characteristics. These systems support a hierarchical, vertical military chain of command structure. They were not designed to support joint operations and are therefore limited when information requirements are based on horizontal or functional sources. The current infrastructure inhibits interoperability necessary to give commanders a unified picture of the battlespace, reduces ability to provide links between the battlefield and the support base, and limits connection to the U.S. industrial base.

One part of the Defense Information Infrastructure plan is to establish a common operating environment that provides integrated support services and corresponding software for standard functional applications. The idea for the common operating environment originated with an observation about command and control systems. Certain functions (mapping, track management, and communication interfaces, for example) are so fundamental that they are required for virtually every command and control system. Yet, in stand-alone systems across DOD, these functions are built over and over again in incompatible ways, even when the requirements are the same or vary only slightly between systems. The common operating environment is intended to standardize the underlying computing infrastructure used to process information. It is to improve interoperability by creating architecture principles that, if adhered to, will allow for the sharing of software products and services and information across the Defense Information Infrastructure. Both the Defense Information Infrastructure plan and the common operating environment are long-term strategies that extend through the year 2010.

Finally, DOD's 1993 Levels of Information Systems Interoperability initiative is to improve C4 and intelligence systems' interoperability. System developers are to use this tool to assess interoperability, determine capabilities needed to support system development, and determine the degree of interoperability needed between C4I and other systems. The tool has not yet been fully tested or implemented. Major testing is planned for July 1998.

Concerns regarding the success of some of these initiatives have been expressed by various DOD organizations. Specifically, in its June 1996 report, the DOD Integration Task Force stated that compliance with the common operating environment standards will not ensure that systems

Appendix I
DOD Initiatives to Improve the
Interoperability of C4I Systems

will be interoperable because, in part, it does not eliminate the problems of data translation, remapping, and duplication. Further, Test Command officials and others believe the DOD Information Infrastructure and common operating environment requirements need refinement before they can ensure interoperability. For example, these officials believe that the level of compliance with the infrastructure and the common operating environment must be higher than currently required to ensure interoperability. In addition, in a December 1996 report, the Chairman of the Joint Chiefs of Staff listed several challenges to achieving interoperability through DOD's initiatives, including security of the infrastructure, overall integration of the DOD organizations into a common operating environment, and the lack of a formal enforcement mechanism to ensure the services conform to the standards.

Comments From the Department of Defense



COMMAND, CONTROL,
COMMUNICATION
AND INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

February 25, 1998



Mr. Mark E. Gebicke
Director, Military Operations
and Capabilities Issues
National Security and
International Affairs Division
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Gebicke:

This is the Department of Defense (DoD) response to the General Accounting Office Draft Report, "JOINT MILITARY OPERATIONS: Many Command and Control Systems Not Certified as Interoperable," dated January 23, 1998 (GAO Code 703179/OSD Case 1525).

The DoD generally concurs with all GAO recommendations with comments (enclosure). Technical comments are also enclosed to enhance the accuracy of the GAO report. A number of efforts are already underway to improve the Department's Interoperability Certification Process.

The Interoperability Certification process is an extremely challenging effort and many of the Department's management tools and processes for its administration are still evolving. DoD is firmly committed to interoperability and will continue to manage and improve the certification process.

The DoD appreciates the opportunity to comment on the GAO draft report.

The point of contact for this report is COL James Weilbrenner, (703) 697-6726, who is assigned to the Deputy Assistant Secretary of Defense (Command, Control and Communications).

Sincerely,

Anthony M. Valletta
Acting Principal Deputy Assistant Secretary
of Defense (C3I)

Enclosures



GAO DRAFT REPORT DATED JANUARY 23, 1998
(GAO CODE 703179) (OSD CASE 1525)

**"JOINT MILITARY OPERATIONS: MANY COMMAND AND CONTROL SYSTEMS
NOT CERTIFIED AS INTEROPERABLE"**

**DEPARTMENT OF DEFENSE COMMENTS TO
THE GAO RECOMMENDATIONS**

RECOMMENDATION 1: In order to ensure that systems critical to effective joint operations do not proceed to production without due consideration given to the need for interoperability certification, the GAO recommended that the Secretary of Defense require the acquisition authorities to adhere to the requirement that command, control, communications, computers, and intelligence (C4I) systems be tested and certified for interoperability prior to the production and fielding decision unless an official waiver has been granted. (p. 16/GAO Draft Report)

DoD RESPONSE: Concur. The basic policy and procedure documents requiring C4I systems certification testing for interoperability currently exist. Their adequacy in terms of clarity, enforcement, and integration of effort to achieve interoperability requires improvement. These documents include:

DoD Directive 4630.5, "Compatibility, Interoperability, and Integration of C3I Systems."

DoD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of C3I Systems."

DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs."

CJCS Instruction 6212.01A, "Compatibility, Interoperability, and Integration of C4I Systems."

In addition, three of the above documents are currently under revision, and efforts will be made to improve the shortcomings. The fourth document is scheduled to be reviewed shortly. This will also serve to elevate the priority given to certification testing when it competes for funding resources which are always constrained and usually inadequate to

Now on p. 12.

Appendix II
Comments From the Department of Defense

accomplish all of the various requirements. The Services often have to decide whether assigning resources to satisfy testing requirements is the best use of these resources. In making this decision, the Services assess whether modifications made to a system put interoperability at risk. If the risk is minimal, the Services may choose to apply these resources to higher priority efforts in lieu of interoperability testing. The revision of the aforementioned documents should result in improvements in the administrative tracking of systems requiring certification testing and assist the acquisition community to focus on both the resources and required planning when reviewing the Test and Evaluation Master Plans (TEMP).

RECOMMENDATION 2: To improve the process for certifying C4I systems for interoperability, the GAO recommended that the Secretary of Defense, in conjunction with the Chairman of the Joint Chiefs of Staff, direct the Service Secretaries, in collaboration with the Defense Information Systems Agency (DISA) Director, to verify and validate all C4I data in its Defense Integration Support Tool and develop a complete and accurate list of C4I systems requiring certification. (p. 16/GAO Draft Report)

Now on p. 13.

DoD RESPONSE: Concur. The DoD is currently working to improve the accuracy and utility of the Defense Information Support Tool (DIST). Additional work is required to create another field for each system in the DIST which would indicate if the system requires interoperability certification. Once the field is created and the appropriate data populated, then the DIST would be able to generate a report showing systems requiring certification.

RECOMMENDATION 3: Also to improve the process for certifying C4I systems for interoperability, the GAO recommended that the Secretary of Defense, in consultation with the Chairman of the Joint Chiefs of Staff, direct the DISA Director to ensure that the status of system's certification is added to the Defense Integration Support Tool and properly maintained to better monitor C4I systems for interoperability compliance. (p. 16/GAO Draft Report)

Now on p. 13.

DoD RESPONSE: Concur. Interoperability Certification fields have recently been added to the DIST. The content options of the field include Full Certification, Limited Certification, and No Certification. In addition, there is a "Certification Comments" field where information relating to why the system did not achieve Full Certification may be entered. The DIST also

Appendix II
Comments From the Department of Defense

provides "Certified By" and "Certification Date" fields. The JITC has provided DIST personnel with the past four years of certification information for entry into the DIST and is providing quarterly reports of new systems certified in order to maintain accuracy of the DIST.

RECOMMENDATION 4: Also to improve the process for certifying C4I systems for interoperability, the GAO recommended that the Secretary of Defense request that the Chairman of the Joint Chiefs of Staff direct the Joint Staff (in collaboration with the Commanders in Chief, the Services, and the Director, DISA) to develop a process for prioritizing C4I systems for testing and certification. (p. 16/GAO Draft Report)

DoD RESPONSE: Concur. The DoD agrees with the need for prioritization. The JITC will test and certify in accordance with the priorities established by this process. The JITC can raise test scheduling and resource conflicts to the Interoperability Test Panel (ITP) of the Military Communications-Electronics Board (MCEB) for resolution.

RECOMMENDATION 5: Also to improve the process for certifying C4I systems for interoperability, the GAO recommended that the Secretary of Defense request the Chairman of the Joint Chiefs of Staff direct the Joint Staff (in collaboration with the Commanders In Chief, the Services, and the Director, DISA) to develop a formal process to follow-up on interoperability problems observed during exercises, report the problems to the relevant DoD organization, and inform organizations that the systems are required to be tested for interoperability. (p. 16/GAO Draft Report)

DoD RESPONSE: Concur. The DoD agrees with the need to develop a formal process to follow up on interoperability issues learned during exercises. The Joint Universal Lessons Learned System (JULLS) database along with Service and Command Lessons Learned databases are potential sources to acquire this information. The Department also recognizes the need to track the resolution of joint interoperability lessons learned problems to ensure they are adequately addressed by appropriate organizations.

RECOMMENDATION 6: To improve DoD's information on the status of waivers from interoperability certification, the GAO recommended that the Chairman of the Joint Chiefs of Staff establish a system to monitor waivers. The GAO further recommended that the system should inform DoD organizations when waivers expire and request that they either seek an extension of the waivers or

Now on p. 13.

Now on p. 13.

Appendix II
Comments From the Department of Defense

test their systems for interoperability. (p. 17/GAO Draft Report)

DoD RESPONSE: Concur. The Joint Staff intends to revise the charter of the MCEB's Interoperability Test Panel to require a quarterly review of all active testing waivers.

Now on p. 13.

Major Contributors to This Report

National Security and
International Affairs
Division, Washington,
D.C.

Carol R. Schuster
Reginald L. Furr, Jr.
Mae F. Jones

Los Angeles Office

George Vindigni
Yelena K. Thompson
David G. Hubbell