United States General Accounting Office

GAO

Report to the Secretary of Defense

June 2001

COMBAT IDENTIFICATION SYSTEMS

Strengthened Management Efforts Needed to Ensure Required Capabilities

GAO-01-632

Contents

Figures

Abbreviations

DOD Department of Defense
C4ISR Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
NATO North Atlantic Treaty Organization
OMB Office of Management and Budget

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

June 25, 2001

The Honorable Donald H. Rumsfeld
The Secretary of Defense

Dear Mr. Rumsfeld:

Friendly fire, or fratricide, incidents accounted for about 24 percent of U.S. fatalities during Operation Desert Storm in 1991. Following that operation, the Department of Defense (DOD) and the military services have been working to find new ways to avoid friendly fire in joint and coalition operations. Their efforts have focused on developing new equipment and technologies as well as new tactics, training, techniques, and other solutions.

In particular, DOD and the military services have been working toward developing a group, or family, of systems that can effectively work together to improve the military's ability to prevent friendly fire. These range from systems that can query and identify a specific target as "friendly" or "unknown," to situational awareness systems that rely on periodic updates of position data to help users locate friendly forces. They would be used in surface-to-surface, air-to-surface, air-to-air, and surface-to-air operations. And they would be equipped on aircraft, surface vehicles, air traffic control stations, as well as weapon systems carried by ground troops.

Effectively managing such a large and complex endeavor requires, among other things, a well-defined and enforced blueprint for operational and technological change, commonly referred to as an enterprise architecture. 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—architectures help ensure that new systems are compatible, interoperable, and supportive of long-term plans.

Because of the importance of an enterprise architecture to effective systems development, we reviewed DOD's efforts to develop and implement one for combat identification. We also reviewed DOD's efforts to establish the management structures and processes needed to ensure that new systems can operate jointly and with U.S. allies.

Results in Brief

DOD does not have an enterprise architecture to guide its effort to develop combat identification systems. While it has initiated efforts to develop one, they have not been comprehensive or adopted by the military services. DOD began an effort in 1994, for example, to develop a systems architecture, but it did not define the operational elements activities, tasks, and information flows required to accomplish combat identification functions. It also did not define technical standards and rules governing the arrangement and interaction of combat identification systems. And, it did not address future needs and capabilities. A subsequent effort that began in 2000 would exclude air-to-air and surface-to-air operations and DOD has yet to develop specific tasking plans for defining systems and technical architectures. In addition, the effort has not been fully funded.

DOD also does not yet have the management structure and processes that are required to ensure that combat identification systems developed across the department are compatible and interoperable, not duplicative, and are in-line with overall department goals. Such mechanisms would include specifically defined focal points responsible for coordinating development efforts; plans that lay out specific initiatives, programs, and projects needed to achieve DOD's combat identification goals; procedures for defining such things as system requirements, procuring systems, and funding specific efforts; and performance measures. Again, DOD has initiated efforts to develop a management framework, including a 1993 initiative that created a focal point for all combat identification activities and defined an acquisition strategy. However, these are no longer in use. Moreover, needed actions in the Joint Chiefs of Staff's combat identification action plan have not been fully funded.

Our experience with federal agencies has shown that attempting to define and build major systems without first completing an enterprise systems architecture often results in systems that are duplicative, not well integrated, unnecessarily costly to maintain and interface, and do not effectively optimize mission performance. Moreover, without good management controls, agencies are not able to ensure efforts are sufficiently coordinated and funded. Some of these problems have already occurred in DOD. Consequently, we are making recommendations to strengthen DOD's management of its combat identification efforts to help ensure attainment of required capabilities.

In commenting on a draft of this report, DOD agreed with all of our recommendations and cited ongoing and planned initiatives to address our concerns.

Background

Friendly fire is a serious problem confronting DOD and the military services. According to a report issued by the Office of Technology Assessment in 1993,[1] about 24 percent of the fatalities experienced during Operation Desert Storm were the result of friendly fire—a rate that appeared very high compared to past conflicts. Sixty-one percent of these incidents involved ground-to-ground incidents, while air-to-ground and ground-to-air incidents accounted for 36 and 3 percent, respectively. A more recent notable incident is the 1994 friendly forces' shootdown of two Blackhawk helicopters over Iraq during Operation Provide Comfort.[2] Such incidents may be caused by command and control failures, navigation failures, or target misidentification.

A key aspect of DOD's effort to prevent friendly fire is the development of new combat identification systems. Some of these systems will "cooperate" to identify friendly targets through queries and answers. Others will identify targets as friendly or unknown with the help of data sources, such as radio emissions or acoustic signals. And others, known as situational awareness systems, will rely on periodic updates of position data to help users locate friendly forces. The cost of such systems is significant. For example, the Army's efforts to develop, field, and maintain cooperative combat identification systems alone are expected to cost more than $1 billion.

Successfully developing and implementing these systems is a major challenge for DOD. The systems themselves will be developed and managed by many different entities within DOD and the military services. They will be involved in a wide range of military operations and installed on a broad array of equipment. At the same time, however, these systems will need to be compatible and interoperable. They will also need to fit in with DOD's long-term goals for achieving information superiority over the enemy. DOD defines this as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Additionally, it is important that these systems be able to work with systems belonging to North

[1] U.S. Congress, Office of Technology Assessment, *Who Goes There: Friend or Foe?,* OTA-ISC-537 (Washington, DC; U.S. Government Printing Office, June 1993).

[2] Operation Provide Comfort, which began April 5, 1991 and ended on December 31, 1996, combined the efforts of four nations—the United States, United Kingdom, France and Turkey—to provide a security force for the 3.2 million people in northern Iraq, a deterrent force against Iraqi aggression and a humanitarian relief effort.

Atlantic Treaty Organization (NATO) and other allies in order to help preclude friendly fire incidents during coalition operations.

DOD Lacks Architecture for Combat Identification

DOD does not yet have a complete enterprise architecture to guide its efforts to develop a family of combat identification systems and past attempts to establish an architecture were not comprehensive or adopted by the services. Without a "blueprint" to guide and constrain DOD's investments in combat identification systems, the military services and Defense agencies may well find themselves with combat identification systems that are duplicative, not interoperable, and unnecessarily costly to maintain and interface.

Value of an Enterprise Architecture

An enterprise architecture systematically captures in useful models, diagrams, and narrative the full breadth and depth of the mission-based mode of operations for a given enterprise, which can be (1) a single organization or (2) a functional or mission area that transcends more than one organizational boundary (e.g., financial management, acquisition management, or combat identification). Further, such an architecture describes the enterprise's operations in both (1) logical terms, such as interrelated functions, information needs and flows, work locations, and system applications, and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards.

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 major systems without first completing an enterprise systems architecture often results in systems that are duplicative, not well integrated, unnecessarily costly to maintain and interface, and do not effectively optimize mission performance.

The Office of Management and Budget (OMB) has recognized the importance of agency enterprise architectures. OMB has issued guidance that, among other things, requires agency information system investments to be consistent with agency architectures.[3] More recently, the Chief

[3] OMB Memorandum M-97-02, *Funding Information Systems Investments*, October 25, 1996, and OMB Memorandum M-97-16, *Information Technology Architectures*, June 18, 1997.

Information Officers Council produced guidance for federal agencies in initiating, developing, using, and maintaining enterprise architectures.[4]

DOD has also issued architecture policy, including a framework defining an architecture's structure and content. Specifically, in February 1998,[5] DOD directed its components and activities to use the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework, Version 2.0. DOD's framework is comprised of three components: (1) an operational architecture—that is, the operational elements, activities, tasks, and information flows required to accomplish or support a mission, (2) a systems architecture—that is, the systems and interconnections supporting the functional mission, and (3) a technical architecture—that is, the minimum set of standards and rules governing the arrangement, interaction, and interdependence of systems applications and infrastructure.

According to DOD, the C4ISR Architecture Framework is a critical tool for achieving its strategic direction and all DOD components and activities should use the framework for all functional areas and domains within the Department. The C4ISR Architecture Framework is recognized in the Federal Chief Information Officers Council's *A Practical Guide to Federal Enterprise Architecture* as a model architecture framework for developing enterprise architectures. Appendix I provides more detailed information on the C4ISR Architecture Framework.

DOD has also recognized the importance of architectures in its recently revised acquisition guidance, DOD Directive 5000.1 and Instruction 5000.2. This guidance sets DOD policy for managing all acquisition programs. Among other things, it requires the use of architectures to characterize the interrelationships and interactions between U.S., allied, and coalition systems.

[4] Chief Information Officers Council, *A Practical Guide to Federal Enterprise Architecture, Version 1.0*, February 2001.

[5] The February 28, 1998, memorandum was jointly signed by the Under Secretary of Defense (Acquisition and Technology), the Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director for C4 Systems, Joint Chiefs of Staff.

DOD Still Lacks a Complete Architecture for Combat Identification

DOD has initiated efforts to develop an architecture for combat identification, but they have not been comprehensive or adopted by the military services. The first effort began in 1994 with the creation of a Combat Identification Task Force. Among other things, such as identifying promising combat identification technologies for a planned demonstration, the Task Force sought to develop an overall architecture for combat identification through an architecture working group. However, this effort only focused on specific systems and how they would work together. It did not define the operational elements and activities required to support a future warfighting vision or technical standards. Both views are integral to an overall architecture. According to DOD, for example, the operational view is useful for facilitating a number of actions across DOD, such as defining operational requirements to be supported by physical resources and systems. The technical view enables interoperability and compatibility of systems, by providing the standards, criteria, and reference models upon which engineering specifications are based, common building blocks are established, and applications are developed.

The work of the architecture working group also excluded elements integral to the battlefield, such as dismounted soldiers, ships, air defense sites, and air-to-ground missions other than close-air support. Additionally, the architecture developed only dealt with the need to identify forces as being either friendly or hostile. It did not address the need to further distinguish targeted systems by class (e.g., "tank" vs. "truck"), platform (e.g., MIG 29 vs. T-72 Main Battle Tank) or intent (e.g., a defecting vs. an attacking platform). More critically, the architecture was never adopted by the services.

Subsequent work began in January 2000 when the Joint Chiefs of Staff's Combat Identification Assessment Division began planning draft guidance on an effort to analyze alternative current and evolving combat identification technologies to support development of an operational architecture. The analysis is expected to take over 2 years to complete at an estimated cost of $10 million. However, this effort is to focus on surface-to-surface and air-to-surface military operations and not to include air-to-air or surface-to-air operations. While the draft guidance for the analysis indicated that the Army should lead the effort with support from the other services, thus far, only the Air Force has budgeted funds—$2 million—toward accomplishing this task. Similarly, in January 2001, the Assessment Division described efforts to develop the operational architecture itself. However, this effort is currently unfunded. According to DOD officials, the reasons for the current lack of funding include the

difficulty of reflecting such efforts in DOD's budgets in a timely manner and addressing competing service funding priorities.

Lack of an Architecture Poses Significant Risks

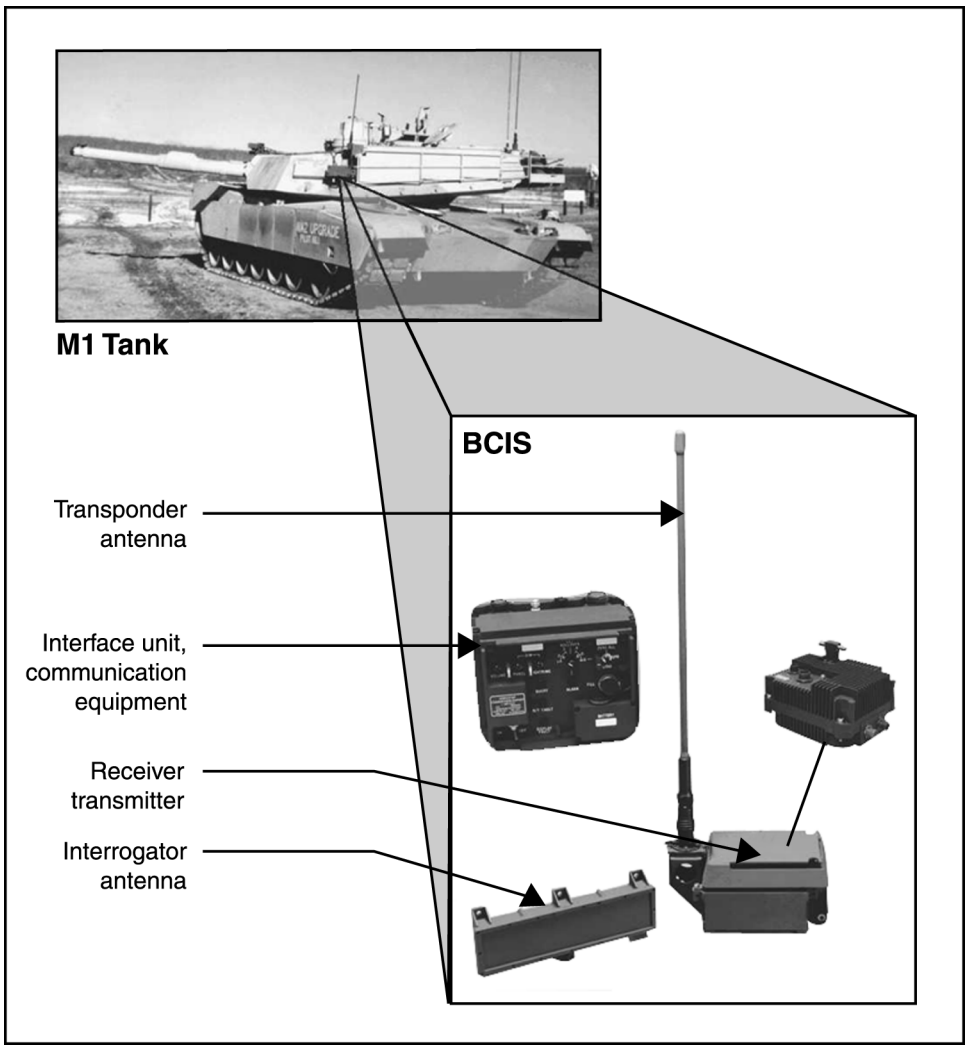
Architectures enable organizations to know their portfolio of desired systems and to develop a clear understanding of how these systems will collectively support and carry out their objectives. Moreover, they help ensure that systems are interoperable, function together effectively, and are cost-effective over their life cycles. Our previous reviews at the Federal Aviation Administration, Customs Service, Department of Education, Internal Revenue Service, Bureau of Indian Affairs, and National Oceanic and Atmospheric Administration have shown that while the absence of a complete architecture does not guarantee the failure of system modernization efforts, it does greatly increase the risk that agencies will spend more money and time than necessary to ensure that systems are compatible and in line with business needs.[6]

Our previous work reviewing DOD's combat identification efforts has shown that DOD is confronting such risks. In 1993, we reported[7] on the Army's ongoing efforts to develop its Battlefield Combat Identification System (see fig. 1)—a system designed to provide a ground-to-ground and potentially an air (helicopter)-to-ground cooperative identification capability. We found that the Army planned to spend up to $100 million on a near-term combat identification system even though the system might eventually be discarded if it could not be integrated into a long-term solution. We also reported that the Army planned to eventually buy 1,520 of the near-term systems to equip some forces even though that number would not be sufficient for a larger-scale operation.

[6] *Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization* (GAO/AIMD-97-30, Feb. 3, 1997); *Customs Service Modernization: Architecture Must Be Complete and Enforced to Effectively Build and Maintain Systems* (GAO/AIMD-98-70, May 5, 1998); *Student Financial Aid Information: Systems Architecture Needed to Improve Program's Efficiency* (GAO/AIMD-97-122, July 29, 1997); *Tax Systems Modernization: Management and Technical Weaknesses Must Be Corrected If Modernization Is to Succeed* (GAO/AIMD-95-156, July 26, 1995); *Weather Forecasting: Systems Architecture Needed for National Weather Service Modernization* (GAO/AIMD-94-28, Mar. 11, 1994); *Indian Trust Funds: Interior Lacks Assurance That Trust Improvement Plan Will Be Effective* (GAO/AIMD-99-53, Apr. 28, 1999).

[7] *Minimizing Friendly Fire: The Army Should Consider Long-Term Solution in Its Procurement Decision on Near-Term Needs* (GAO/NSIAD-94-19, Oct. 22, 1993).

Figure 1: The Battlefield Combat Identification System



Source: U.S. Army.

Additionally, absent the understanding provided by an enterprise architecture, the services risk being unable to effectively define and develop weapon system requirements (e.g., system characteristics, functions, and performance parameters). As mentioned earlier, developing an enterprise architecture provides further understanding of (1) the operational elements, activities, tasks, and information flows needed to accomplish a mission, (2) the systems needed and their interconnections to support that mission, and (3) the minimum set of standards and rules

needed to govern their arrangement, interaction, and interdependence. As a result, systematically reviewing specific systems' requirements within the context of such an architecture can help ensure the development of cost-effective systems to provide needed capabilities.

DOD has already identified some broader needs for combat identification. Specifically, in 1992 and again in 1998, DOD defined its overall mission needs for combat identification systems and it defined the capabilities it expected from these systems, including

- positive, timely, and reliable identification of friends, foes, and neutrals;[8]
- classification of foes by platform, class/type, and nationality; and
- friend-from-friend discrimination.

More recently, the U.S. Joint Forces Command developed a Capstone Requirements Document that defines overarching requirements for the combat identification family of systems.

Lastly, without having a complete architecture for combat identification, DOD may not be able to ensure that its own operational, systems, and technical requirements are aligned with those of NATO allies. NATO is currently developing both an operational architecture and a systems architecture in all mission domains (air-to-air, surface-to-air, air-to-surface, and surface-to-surface). It plans to complete these architectures by the end of 2001 and the end of 2002, respectively. If DOD's efforts to develop an enterprise architecture for combat identification occur in a timely manner, they could be more closely aligned with NATO's efforts and possibly improve coalition interoperability. Moreover, DOD would be able to ensure that the long-term capabilities it envisions for combat identification are recognized.

[8] DOD has further clarified this by stating that "friendly includes military allies and coalition partners" and the neutral "includes non-aligned military forces and non-combatants."

Important Management Tools for Developing Combat Identification Systems Needed

The effort to develop new systems for combat identification is challenging not only because the systems themselves span a number of entities within DOD but also because they may need to operate jointly and with systems belonging to allies and work in concert with DOD's long-term goals for information superiority. DOD's success, therefore, hinges on having effective management structures and processes—e.g. focal points, funding and development plans, schedule and resource estimates, performance measures, progress reporting requirements—to guide and manage systems development.

DOD and the services have established focal points for coordinating combat identification efforts. For example, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence is responsible for overseeing combat identification programs and the Joint Chiefs of Staff has ongoing efforts to improve combat identification capabilities. However, DOD currently lacks a formalized framework defining the procedures and controls that would facilitate these efforts. As a result, coordination and funding of development initiatives is not assured.

Management Structures and Controls Needed to Guide System Development

Because the prevention of friendly fire is a DOD-wide effort involving the military services, other DOD components, and even U.S. allies, it must be approached as an enterprise endeavor with senior executive management sponsorship. This requires identifying an entity or individual with organizational authority, responsibility, and accountability for managing system development as an agencywide project and ensuring appropriate resources are provided to accomplish needed tasks and develop required systems.

We have reported on the need for cohesive management in developing combat identification systems in the past. In 1995, we issued a report[9] on Army and Navy-led efforts to develop cooperative identification systems. We found that the Army and Navy were pursuing development of systems without having developed a cohesive management plan and organizational structure and made recommendations to strengthen those efforts.

[9] *Combat Identification Systems: Changes Needed in Management Plans and Structure* (GAO/NSIAD-95-153, Sept. 14, 1995).

Given the size and complexity of the project, it is important for DOD to have a plan that lays out the current combat identification capabilities, desired capabilities, and specific initiatives, programs, and projects intended to get DOD and the services to that vision. Such plans, or roadmaps, are often developed as part of an enterprise architecture. To facilitate the implementation of these plans, it is also necessary for DOD to define the organizational structure, responsibilities, and procedures for such things as defining system requirements, developing and procuring systems, and funding specific efforts. Together, these structures and processes can help ensure that combat identification projects are not duplicative or disparate and that they receive adequate priority and funding.

Lastly, it is important that DOD define performance measures to assess the progress of combat identification improvements. The Government Performance and Results Act of 1993[10] requires federal agencies and activities to clearly define their missions, set goals, link activities and resources to goals, prepare annual performance plans, measure performance, and report on their accomplishments.

Performance measures can be particularly helpful in ensuring that services and components are effectively coordinating their development efforts. For example, DOD could measure the progress associated with planning and successfully conducting joint, cross-service, and allied demonstrations of interoperable systems. Performance measures can also help ensure projects are adequately funded, for example, by measuring whether the services' budgets support efforts to develop an enterprise architecture for combat identification.

Past Efforts That Sought to Ensure Cohesiveness No Longer in Use

DOD has recognized the benefit of formally defining management structures and processes in the past to guide combat identification efforts, but those efforts are no longer in use.

First, in January 1993, the services signed a Memorandum of Agreement on Joint Management of Combat Identification to coordinate and provide oversight of their requirements, policies, procedures, development and procurement programs, and related technology efforts. The agreement stated that combat identification encompasses widely varying

[10] Public Law 103-62, August 3, 1993.

requirements, policies, platforms, mission areas, and technologies. Among other things, the agreement created a General Officer Steering Committee to serve as a primary focal point for all DOD combat identification activities; a Joint Combat Identification Officer under that committee to provide lower-level coordination on all DOD efforts and develop a master plan for combat identification efforts; three supporting committees; and two acquisition-related groups.

Following the agreement, DOD published a joint master plan for its "cooperative identification" system development efforts (that is, systems that identify friendly or unknown through queries and answers). The plan defined management strategies and structures to plan and execute these technologies and it defined an acquisition strategy that called for such things as baselining existing capability, identifying and prioritizing deficiencies, coordinating advanced research and development activities, and integrating system architectures.

However, the memorandum of agreement is no longer in use and only one of the entities created from the memorandum still exists—the Joint Chiefs of Staff's Combat Identification Assessment Division (formerly the Joint Combat Identification Office). Moreover, according to a DOD official, the Joint Master Plan for cooperative systems development is no longer in use because the services' efforts did not evolve into joint programs as originally envisioned.

In 1996, the services developed another master plan that represented their strategic vision for developing, maintaining, and enhancing their combat identification capability. This plan went beyond the 1993 plan by including noncooperative and situational awareness system development efforts. The plan was to serve as the focal point for coordination of joint and service-unique initiatives during the budget process. However, it was updated only once in 1998 and that revision was never adopted by the department.

Since then, the Joint Chiefs of Staff's Combat Identification Assessment Division has developed and updated an annual action plan. Many of the plan's tasks are designed to address known deficiencies that can be corrected in the near term. The plan does not define management structures and procedures for guiding system development. And, while it does call for a semiannual report on progress, it does not define specific measures to be used in assessing that progress. Moreover, the Assessment Division does not have authority to direct the services to implement its plan nor does it have funding authority of its own to carry out the plan's

tasks. Rather, an Assessment Division official stated that the services' cooperation is essential to implement the plan.

Development Efforts Have Not Been Effectively Coordinated or Sufficiently Funded

Without sufficient structures and processes to coordinate and guide systems development, some combat identification projects have not been sufficiently funded. For example, as mentioned earlier, the systems analysis DOD planned to support development of an operational architecture for combat identification has an estimated cost of $10 million. However, while the guidance for this analysis indicated that the Army should lead the effort with support from the other services, thus far only the Air Force has budgeted funds—$2 million—toward its accomplishment. In addition, the Combat Identification Assessment Division's planned operational architecture is also unfunded at this time.

Similar problems are occurring at the service level. Based on a review of the Battlefield Combat Identification System program, the DOD Inspector General recently reported[11] that the Army has obligated $132.4 million in research, development, test and evaluation, and procurement funds through fiscal year 2000 and plans to obligate another $86.5 million to complete development efforts and procure 1,169 low-rate initial production systems from fiscal year 2001 through fiscal year 2007 for the 4th Infantry Division. However, the Inspector General also reported that the Army has not provided $918.5 million of procurement and operations and maintenance funds for the program's procurement objective of 16,414 systems.[12]

The lack of a management framework also makes it difficult to coordinate projects among the services to ensure that they are not redundant or disparate. For example, the Army recently proposed a memorandum of agreement between the Army and the Marines for cooperation in battlefield identification activities. The memorandum was to describe the activities and intentions of the two services to promote and ensure joint operational interoperability and to encourage sharing of information and

[11] *Acquisition of the Battlefield Combat Identification System*, Department of Defense, Office of the Inspector General, Audit Report D-2001-093, March 30, 2001.

[12] DOD's acquisition guidance now addresses the risk involved in such incidents by requiring that programs be fully funded (i.e., inclusion in the budget and out-year program of the funding for all current and future efforts necessary to carry out the acquisition strategy) before they transition into system development and demonstration.

joint work on combat identification concepts, doctrine (tactics, techniques, and procedures), experimentation, operational analysis, and lessons learned. The proposed agreement was also to acknowledge that the Army was pursuing its Battlefield Combat Identification System for ground-to-ground identification and that the Marines' priority of effort would go toward air-to-ground identification.

The Marines declined the Army's proposed agreement. A Marine Corps official told us that the recent approval of a NATO Standardization Agreement for battlefield identification systems mandating the use of the same technology employed in the Army's system[13] and the development of the recently approved combat identification Capstone Requirements Document negate the need for a separate agreement to address interoperability between Army and similar Marine Corps systems. Complying with the NATO agreement and the Capstone Requirements Document may enable the Marines to build systems that can interact with those built to NATO's standards and that have the capabilities that DOD has envisioned. However, it reduces assurance that Marine systems will be fully interoperable with the Army's and it will not reduce the risk of inefficient redundancy of service efforts.

Conclusions

Preventing friendly fire is a complex and challenging endeavor. It encompasses the development of new technologies as well as new training, tactics, and warfighting techniques. It involves a range of equipment and systems that have historically not been able to effectively interact as well as a variety of military operations. And it's a concern among each of the services as well as our allies. Clearly, it is essential to have a blueprint that ties together these elements and provides a comprehensive map for long-term improvements as well as a management framework that is strong enough to implement the blueprint. While DOD has taken some concrete steps toward both ends, it needs to strengthen these efforts and ensure that they are supported by the services. Without doing so, it may well continue to contend with problems leading to friendly fire incidents.

[13] The Army's current Battlefield Combat Identification System will require some modifications to become compliant with the standardization agreement.

Recommendations for Executive Action

To improve DOD's combat identification system development efforts, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, in collaboration with the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Joint Staff's Combat Identification Assessment Division; and the services; to

- Develop—in accordance with federal guidelines and relevant DOD policies and guidance—an enterprise architecture for combat identification that reflects the needs of its future warfighting vision. The architecture should define (1) the operational elements, activities, tasks, and information flows required to accomplish the combat identification mission, (2) the systems and interconnections supporting the mission, and (3) the minimum set of standards and rules governing the arrangement, interaction, and interdependence of systems applications and infrastructure. It should also encompass air-to-air, surface-to-air, surface-to-surface, and air-to-surface operations. Once the architecture is defined, we recommend that DOD review specific system requirements to determine whether they should be adjusted to address the needs reflected in those architectures or determine if gaps exist and new development efforts are needed.
- Develop and annually update a written, formalized management framework to guide the department's combat identification efforts. The framework should define the organizational structure and procedures to be used in managing those efforts including the structures and procedures to coordinate requirements' and systems' development and funding, and develop and enforce the enterprise architecture. Until an enterprise architecture is developed, the framework should contain interim procedures for the review of ongoing efforts and that allow continuation of only efforts deemed essential or for which risk mitigation mechanisms have been provided. The framework should also provide roadmaps to future developments and define time-phased measures of program performance.

In addition, to enable accomplishment of overarching combat identification efforts, we recommend that the Secretary of Defense ensure that adequate funding is provided to implement these initiatives.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD agreed with all three of our recommendations and cited ongoing and planned initiatives to address our concerns. We are encouraged by the department's initiatives.

In concurring with our recommendation related to the development and use of an enterprise architecture, DOD stated that two of the three views forming that architecture—the operational and systems views—are to be developed in the near-term. The department added—as we recommended—that these views can then be used as a guide to review and adjust systems requirements and to determine if gaps exits that may require new development efforts. DOD also stated that development of the technical architecture view will be initiated once development of the other views has progressed to an appropriate point.

DOD agreed with our recommendation that the department develop and annually update a written, formalized management framework to guide its combat identification efforts. DOD commented that it has a formalized framework to guide its combat identification efforts that is delineated in a draft Joint Staff Combat Identification Assessment Team charter, the Joint Staff Combat Identification Action Plan, and a Combat Identification Capstone Requirements Document. To complement the Joint Staff's efforts, DOD proposes the establishment of a combat identification integrated product team to assist in developing and enforcing the combat identification systems architecture and resolving combat identification system acquisition, integration, and synchronization issues. Also, the team is to produce roadmaps and time-phased measures of program performance for individual system's development efforts as required.

DOD stated that it agreed with our recommendation regarding the need for adequate funding of overarching combat identification efforts. The department commented that it is committed to the identification of funding to support these efforts through its budgeting and requirements processes.

DOD's comments are reprinted in appendix II. In addition, DOD also provided technical comments that we incorporated as appropriate.

Scope and Methodology

To determine whether the services are using an enterprise architecture to guide their combat identification efforts, we reviewed documents relating to services' prior, current, and planned combat identification efforts. We also discussed architecture-related issues with officials from the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence; the Joint Chiefs of Staff Combat

Identification Assessment Division; the NATO Identification System Coordination Office; and various service activities. Additionally, we reviewed DOD and Joint Chiefs of Staff guidance on requirements development and examined DOD's and the service's planned actions within the context of that guidance. We also discussed requirements issues with cognizant DOD and service officials.

To determine whether DOD and the services have developed and are using cohesive management plans to assure inter-service and allied interoperability of cost-effective combat identification systems, we reviewed previous combat identification plans and discussed those plans with DOD representatives and the services. We also discussed general management issues with those officials and developed information on management problems that might be avoided by developing a cohesive management plan. Additionally, to gain a better understanding of DOD and allied interoperability requirements, we discussed combat identification issues with representatives of NATO and the United Kingdom's National Audit Office, Ministry of Defence, and Defence Evaluation and Research Agency.

We conducted our work from September 2000 through June 2001 in accordance with generally accepted government auditing standards.

This report contains recommendations to you. As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Governmental Affairs and to the House Committee on Government Reform not later than 60 days from the date of this letter and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this letter.

We are sending copies of this report to the appropriate congressional committees. We are also sending copies to the Honorable Thomas E. White, Secretary of the Army; the Honorable Gordon R. England, Secretary of the Navy; the Honorable James G. Roche, Secretary of the Air Force; General James L. Jones, Commandant of the Marine Corps; the Honorable Mitchell E. Daniels, Jr., Director, Office of Management and Budget; and other interested parties. We will make copies available to others upon request. The report will also be available on our homepage at http://www.gao.gov.

Please contact me at (202) 512-4841 if you have any questions concerning this report. Major contributors to this report were Charles F. Rey, Bruce H. Thomas, Thomas W. Hopp, Rahul Gupta, Hai Tran, Gary L. Middleton, Cristina Chaplain, and Randolph C. Hite.

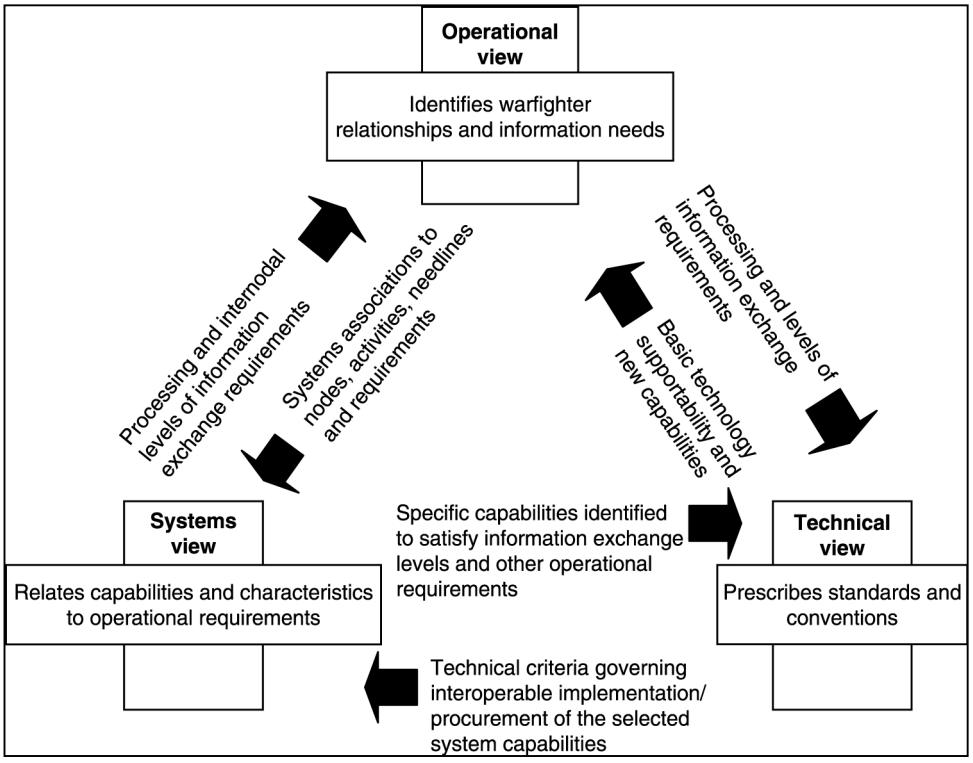
Sincerely yours,

Allen Li
Director, Acquisition
and Sourcing Management

Appendix I: DOD's Enterprise Architecture Framework: A Brief Description

The Department of Defense (DOD) has published a framework for the development and presentation of architectures within DOD.[1] The framework defines the type and content of architectural artifacts, as well as the relationships among artifacts, that are needed to produce a useful enterprise architecture. Briefly, the framework decomposes an enterprise architecture into three primary views (perspectives into how the enterprise operates): the operational, systems, and technical views, also referred to as architectures. According to DOD, the three interdependent views are needed to ensure that information technology systems are developed and implemented in an interoperable and cost-effective manner. Each of these views is summarized below. (Fig. 2 is a simplified diagram depicting the interrelationships among the views.)

Figure 2: Interrelationship of Three Architecture Views



Source: C41SR Architecture Framework, Version 2.0, December 18, 1997.

[1] *C4ISR Architecture Framework, Version 2.0*, December 18, 1997.

- The operational architecture view defines the operational elements, activities and tasks, and information flows required to accomplish or support an organizational mission or business function. According to DOD, it is useful for facilitating a number of actions and assessments across DOD, such as examining business processes for reengineering or defining operational requirements to be supported by physical resources and systems.
- The systems architecture view defines the systems and their interconnections supporting the organizational or functional mission in context with the operational view, including how multiple systems link and interoperate, and may describe the internal construction and operations of particular systems. According to DOD, this view has many uses, such as helping managers to evaluate interoperability improvement and to make investment decisions concerning cost-effective ways to satisfy operational requirements.
- The technical architecture view defines a minimum set of standards and rules governing the arrangement, interaction, and interdependence of system applications and infrastructure. It provides the technical standards, criteria, and reference models upon which engineering specifications are based, common building blocks are established, and applications are developed.

Appendix II: Comments From the Department of Defense

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

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

June 18, 2001

Mr. Allen Li
Director, Acquisition Sourcing and Management
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Li:

This is the Department of Defense (DoD) response to the GAO draft report "COMBAT IDENTIFICATION SYSTEMS: Strengthened Management Efforts Needed to Ensure Required Capabilities," dated May 18, 2001 (GAO Code 707557/OSD Case 3097). DoD comments are enclosed.

The OSD point of contact in this matter is Alan Lahoff, 703-607-0293, who is assigned to the Communications, Command and Control Directorate.

Sincerely,

Robert M. Nutwell, RADM, USN
Deputy Assistant Secretary of Defense
(C3ISR and Space)

Enclosure:
DoD comments

GAO Draft Report, "COMBAT IDENTIFICATION SYSTEMS: Strengthened Management Efforts Needed to Ensure Required Capabilities," Dated May 18, 2001 (GAO Code 707557/ OSD Case 3097)

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

To improve DoD's combat identification system development efforts, the GAO recommended that the Secretary of Defense direct the Assistant Secretary of Defense for Command, Control Communications, and Intelligence, in collaboration with the Office to the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Joint Staff's Combat Identification Assessment Division; and the Services to:

Recommendation 1: Develop- in accordance with federal guidelines and relevant DOD policies and guidance-an enterprise architecture for combat identification that reflects the needs of its future warfighting vision. The architecture should define (1) the operational elements, activities, tasks and information flows required to accomplish the combat identification mission, (2) the systems and interconnections supporting the mission, and (3) the minimum set of standards and rules governing the arrangement, interaction, and interdependence of systems applications and infrastructure. It should encompass air-to-air, ground-to-air, ground-to-ground, and air-to-ground operations. Once the architecture is defined, we recommend that DOD review specific system requirements to determine whether they should be adjusted to address the needs reflected in those architectures or determine if gaps exist and new development efforts are needed. (p. 15/GAO Draft Report)

DoD Response: Concur. We agree with the need for the identified architecture. Two of the views that would comprise the architecture – Operational and Systems views– for combat identification are to be developed in the near term. The Joint Staff's 2001 Combat Identification Action Plan addressed this by calling for an architectural effort. This effort, however, was subsequently tabled pending initial results of strategic topics studies directed by the Joint Requirements Oversight Council. These strategic studies are being undertaken to support the Department's joint warfighting vision, Joint Vision 2020, with interim results planned for release by the first quarter of fiscal year 2002. Therefore, we anticipate that the Action Plan tasking will be initiated in the first quarter of fiscal year 2002 with the goal of deriving a combat identification operational architecture based on the interim operational architectures developed by the strategic studies. Given a first quarter fiscal year 2002 start, the combat identification operational and systems architecture views should then be completed by the second quarter of fiscal year 2003 pending funding availability. These efforts will provide important understanding into our combat identification needs and will closely aligned with NATO.

These architecture views will encompass air-to-air, ground-to-air, ground-to-ground, and air-to-ground operations. The architecture views can then be used as a guide to review and adjust systems requirements and to determine if gaps exist that may require new development efforts. As to the completion of the technical architecture, we intend to initiate development of that architecture once development of the operational and systems architecture views has

progressed to the appropriate point. We believe that when undertaken, the technical architecture view should be developed by the Services' combat identification system program offices due to their familiarity with the appropriate technical standards and engineering specifications. However, the technical architecture view would be developed under oversight of the combat identification Integrated Product Team (IPT) (proposed below) and the Joint Staff Combat Identification Assessment Team.

Recommendation 2: Develop and annually update a written, formalized management framework to guide the department's combat identification efforts. The framework should define the organizational structure and procedures to be used in managing those efforts including the structures and procedures to coordinate requirements' and systems' development and funding, and develop and enforce the enterprise architecture. Until an enterprise architecture is developed, the framework should contain interim procedures for review of ongoing efforts and that allow continuation of only efforts deemed essential or for which risk mitigation mechanisms have been provided. The framework should also provide roadmaps to future developments and define time-phased measures of program performance. (p. 15/GAO Draft Report)

DoD Response: Concur. The Department has a formalized management framework to guide combat identification efforts including the structures and procedures to coordinate requirements' and systems' development and funding and develop and enforce the proposed enterprise architecture. This framework is delineated in the draft Joint Staff Combat Identification Assessment Team charter (under coordination); the Joint Staff Combat Identification Action Plan (updated annually); and the Combat Identification Capstone Requirements Document. The Joint Staff (J-8) Combat Identification Assessment Team continues to raise the visibility of combat identification issues to senior leadership for resolution. This structure has evolved and strengthened since the 1995 GAO report on combat identification and reflects a close and continuous relationship between the Joint Staff, the Office of the Secretary of Defense, the Commanders in Chief, and the Services.

To complement the requirements development and program assessment efforts of the Joint Staff, OSD proposes to establish a combat identification integrated product team (IPT) composed of members from OSD, the Joint Staff, US Joint Forces Command, and the Services' acquisition communities. The written charter and supporting documents for the IPT would define the interested parties and their roles, and include interim procedures for the review of on-going efforts. This IPT would assist in developing and enforcing the combat identification systems architecture and resolving combat identification system acquisition, integration, and synchronization issues. It would produce roadmaps and time-phased measures of program performance for individual systems development efforts as required. The IPT would provide input to the Department's Programming, Planning, and Budgeting System with special emphasis given to help guide the combat identification portion of the Defense Planning Guidance. This IPT would be the acquisition twin to its requirements sibling, the Joint Staff Combat Identification Assessment Team.

Until the proposed combat identification enterprise architecture is developed, combat identification programs will be evaluated in accordance with the charters of the Combat Identification Assessment Team and proposed IPT; the Joint Combat Identification Action Plan;

the Combat Identification Capstone Requirements Document; DoD Directive 5000.1, DoD Instruction 5000.2; and the proposed September 1995 DoD Combat Identification Task Force Architecture

Recommendation 3: In addition, to enable accomplishment of overarching combat identification efforts, we recommend that adequate funding be provided to implement these initiatives. (p. 15/GAO Draft Report)

DoD Response: Concur. The DoD is committed to the identification of funding to support these efforts through the Department's Programming, Planing, and Budgeting System, and Joint Requirements Oversight Council processes.

Prepared by A.R. Lahoff, OASD(C3I)/C3, 703-607-0293

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are also accepted.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St., NW (corner of 4th and G Sts. NW)
Washington, DC 20013

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

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

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

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

- Web site: http://www.gao.gov/fraudnet/fraudnet.htm
- E-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)