INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Acquisition Management of the Defense Counterintelligence Information System

B. DATE Report Downloaded From the Internet: 02/07/02

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 02/07/02**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

February 6, 2002

Acquisition

Acquisition Management of the Defense Counterintelligence Information System (D-2002-046)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C3I)	Assistant Security of Defense (Command, Control, Communications, and Intelligence)
DCIIS	Defense Counterintelligence Information System
MDITDS	Migration Defense Intelligence Threat Data System

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

February 6, 2002

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, DEFENSE INTELLIGENCE AGENCY

SUBJECT: Audit Report on the Acquisition Management of the Defense Counterintelligence Information System (Report No. D-2002-046)

We are providing this report for information and use. We considered management comments on a draft of this in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Charles M. Santoni at (703) 604-9051 (DSN 664-9051) (csantoni@dodig.osd.mil) or Mr. David M. Wyte at (703) 604-9027 (DSN 664-9027) (dwyte@dodig.osd.mil. See Appendix C for the report distribution. The audit team members are listed inside the back cover.

Thomas F. Gimble
Acting
Deputy Assistant Inspector General
For Auditing

Office of the Inspector General, DoD

Report No. D-2002-046 **February 6, 2002**
(Project No. D2001AL-0073)

Acquisition Management of the Defense Counterintelligence Information System

Executive Summary

Introduction. This report discusses the acquisition management of the Defense Counterintelligence Information System. It is one of a series of acquisition management audits addressing DoD information technology systems.

The Defense Counterintelligence Information System is an information technology investment that, when deployed, will standardize core counterintelligence business processes by integrating counterintelligence collections, investigations, operations, analysis and production, and functional services into a joint operational environment. Originally linked with the Defense Intelligence Agency's acquisition of the Migration Defense Intelligence Threat Data System by direction of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), users would be able to review and evaluate counterintelligence information electronically stored in a common database. Before the Assistant Secretary's Director of Counterintelligence withdrew funding for the Defense Counterintelligence Information System in September 2000 due to deployment delays and users' dissatisfaction with delivered software products, the Defense Intelligence Agency had obligated $12 million for its development and deployment between FY 1995 and FY 2000. In addition, the Assistant Secretary provided the Military Departments and DoD Components with $25 million for infrastructure support costs.

Objectives. The overall audit objective was to evaluate the acquisition management of the Defense Counterintelligence Information System. Specifically, the audit determined whether the information technology system was being cost-effectively acquired, monitored, tested, secured, and prepared for deployment and system life-cycle support in accordance with DoD and other applicable guidance. In addition, we evaluated the management control program related to the objective. See Appendix A for a discussion of the audit scope and methodology and the review of the management control program.

Results. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Defense Intelligence Agency had not adequately managed risk in acquiring the Defense Counterintelligence Information System. As a result, the program was discontinued. Because a business need still exists for the automated information system, the Director of Counterintelligence, Office of Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), has restructured the program and plans to invest more than $45 million between FY 2002 and FY 2007 for development, deployment, operation and maintenance. Further, the Director intends to follow a more disciplined acquisition strategy by avoiding and reducing risks that caused deployment delays and users dissatisfaction with the prior acquisition.

Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), in implementing a disciplined acquisition strategy for the reacquired Defense Counterintelligence Information System, establish management controls for translating mission needs into a set of operational requirements; create a structured, integrated system life-cycle plan with cost, schedule and performance goals for measuring progress and projecting results; maintain documentation for continually justifying the selected solution as the best of alternatives; perform continual assessments of acquisition and security risks with planned actions taken to mitigate them; allocate program development and deployment risks between the Government and contractors; maximize use of commercial technology and competition; and prepare and submit quarterly acquisition oversight reports to functional and acquisition Milestone Decision Authorities.

Management Comments. The Director of Counterintelligence, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the report finding and recommendations. A discussion of management comments is in the Finding section of the report, and the complete text of the management comments is in the Management Comments section.

Table of Contents

Background

This report discusses the acquisition management of the Defense Counterintelligence Information System (DCIIS). It is one of a series of acquisition management audits addressing DoD information technology systems.

DCIIS is an information technology investment that, when deployed, will improve the quality, availability, situational awareness, and timeliness of DoD counterintelligence information. Specifically, DCIIS will standardize core counterintelligence business processes by integrating counterintelligence collections, investigations, operations, and production and functional services into a joint operational environment.

In FY 1995, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C3I)] assigned program acquisition and management responsibilities for DCIIS to the Defense Intelligence Agency. Also, the Assistant Secretary directed that DCIIS share common data with other intelligence systems and be integrated into the Defense Intelligence Agency's Migration Defense Intelligence Threat Data System (MDITDS).[1]

In FY 1999, the Defense Intelligence Agency released Version 1.0 of the MDITDS software more than 2 years beyond the date of its promised deployment. The MDITDS software was released with its DCIIS data collection module turned off, because the DCIIS module was not fully developed and required additional functionality for initial operating capability. Further, when a subsequent version of MDITDS slipped beyond its planned deployment, sponsors within the Defense Intelligence Agency lost confidence in the Agency's ability to deliver a consolidated intelligence system and began withdrawing financial support.[2]

In September 2000, the ASD(C3I) discontinued funding the DCIIS acquisition effort when the Defense Intelligence Agency told the Director of Counterintelligence that it would cost an additional $6.4 million to reengineer DCIIS. However, despite the Assistant Secretary's decision, a business need still existed for a joint information system that would gather and report counterintelligence data.

Funds provided to the Defense Intelligence Agency by ASD(C3I) for the DCIIS information technology investment totaled $12 million between FY 1995 and FY 2000. In addition, ASD(C3I) provided the Military Departments and DoD Components with $25 million for DCIIS infrastructure support.

---

[1]MDITDS consolidated 19 legacy systems supporting counterterrorism, indications and warning, and counterintelligence requirements. Access to and from these systems was through secured communication and router network systems, user identifiers, passwords, and electronic certificates. Information security for MDITDS was tested in June 1998, when the Defense Intelligence Agency evaluated the MDITDS architecture for accreditation.

[2]Since FY 1995, the Defense Intelligence Agency has expended over $50 million for the MDITDS modernization and plans to expend about an additional $4.7 million for operating and maintaining deployed threat assessment applications before MDITDS is discontinued in September 2002.

Objective

The overall audit objective was to evaluate the acquisition management of DCIIS. Specifically, the audit determined whether the information technology system was being cost-effectively acquired, monitored, tested, and prepared for deployment and system life-cycle support in accordance with DoD and other applicable guidance. In addition, we evaluated the management control program related to the objective. See Appendix A for a discussion of the audit scope and methodology and the review of the management control program. Also, see Appendix B for specific regulations and directives applicable to acquisitions of automated information systems.

Acquisition of the Defense Counterintelligence Information System Technology Investment

The ASD(C3I) and the Director, Defense Intelligence Agency, had not adequately managed risk in the DCIIS information technology investment because they:

- did not implement project management controls and oversight for cost-effectively acquiring, monitoring, testing, and preparing the information technology acquisition for deployment and system life-cycle support in compliance with Office of Management and Budget and DoD guidance, and

- linked the DCIIS development and deployment to the MDITDS and its database technology.

As a result, the program was discontinued. The Director of Counterintelligence, Office of Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) has restructured the DCIIS acquisition program because a business need still exists for a joint information system that gathers and reports counterintelligence data. Further, the Director intends to follow a disciplined acquisition strategy for system life-cycle development, deployment, operation, and maintenance by avoiding and reducing risks that caused deployment delays and user dissatisfaction with the prior DCIIS acquisition.

Mandatory Guidance

The Office of Management and Budget and DoD provide managers with system acquisition guidance for cost-effectively acquiring, monitoring, testing, and preparing information technology investments for deployment and system life-cycle support and safeguarding information. The ASD(C3I) and the Defense Intelligence Agency did not comply with that guidance when acquiring DCIIS. Program planning and definition was insufficient for determining progress, measuring efficiency and effectiveness, and projecting results. Further, personnel involved with managing and overseeing the DCIIS acquisition lacked the system acquisition skills required to concurrently develop and deploy two information systems that would be linked to a common database. Appendix B describes the guidance relating to DCIIS.

Program Planning and Definition

Documentation for program planning and definition was either incomplete or did not exist for measuring progress, projecting results and determining system effectiveness and suitability. Missing and incomplete documents included the following:

- Mission needs statement,
- Operational requirements documents,
- Acquisition strategy,
- Acquisition program baseline,
- Test and evaluation master plan,
- Life-cycle cost estimates,
- Risk management plan, and
- Software development plan.

As a result, management controls to measure progress and efficiency and to project results did not exist for determining whether DCIIS was cost-effectively acquired, monitored, tested, and prepared for deployment and system life-cycle support.

Mission Need Statement. The ASD(C3I) had not prepared a mission needs statement for DCIIS. However, a need was recognized in October 1995, when the Counterintelligence Business Process Review Committee recommended that DoD standardize and globally communicate counterintelligence information for operations, collections, investigations, analyses, and production. As a result of this recommendation, ASD(C3I) decided to proceed with DCIIS development.

Operational Requirements Document. In response to the Committee's report, the ASD(C3I) established the Defense Counterintelligence Requirements Panel to identify functional counterintelligence requirements and standardize and coordinate counterintelligence practices and policies. However, the documents prepared by the Panel lacked detail. Issues typically addressed in an Operational Requirements Document, such as numbers of systems and subsystems, interoperability, and operations and maintenance, were missing.

Further, an assessment made by the Computer Sciences Corporation[3] found that no single library contained all of the functional requirements. Documentation was co-located with legacy system documentation, developer folders, and other supporting documentation. In addition, when requirements were contractually tasked to developers, subsequent review and validation by users did not always occur before incremental deployment.

[3]Computer Sciences Corporation, "Program Assessment for the Migration Defense Intelligence Threat Data System," March 30, 2000.

Acquisition Strategy. The DCIIS project management office did not have a documented acquisition strategy until FY 1998. Further, the strategy that was prepared by the Defense Intelligence Agency was incomplete. According to the strategy, DCIIS would be developed and deployed following an evolutionary strategy with incremental deliveries for software enhancements.

However, the acquisition strategy document described only one software delivery. It did not address DCIIS life-cycle development, deployment, operation and maintenance, acquisition and security risks, and periodic report submissions for oversight direction, guidance and Milestone Decisions. Further, the document did not discuss contracting to determine the extent of commercial technology and risk sharing between the Government and contractors and the effective use of vendor competition.

Acquisition Program Baseline. Accountability for the DCIIS acquisition did not exist. The ASD(C3I) and the Director, Defense Intelligence Agency, did not establish program baselines for measuring progress and determining program results. As a result, management controls for making cost, schedule, and performance comparisons and computing indexes for projecting results could not be determined for measuring program efficiency and quality effectiveness.

Test and Evaluation Master Plan. The Defense Intelligence Agency did not develop a test and evaluation master plan for DCIIS. Test and evaluation master plans provide a framework for developing detailed test plans and progressively evaluating identified system-critical operational issues for performance effectiveness and suitability. DCIIS was not stressed to determine whether results exceeded thresholds for operational effectiveness, reliability and maintenance.

Tests performed on the DCIIS were designed to demonstrate product functionality, information security, and interoperability. Also, the developers, rather than independent testers, prepared test plans and limited the number of users engaged in the tests. Further, the Defense Intelligence Agency stated in a project management office newsletter that users would not be satisfied with developers' delivered software products. The Agency expected users to find system discrepancies and a need for additional training.

Life-Cycle Cost Estimate. The ASD(C3I) and the Defense Intelligence Agency did not develop life-cycle cost estimates for DCIIS software. Life-cycle acquisition and ownership cost estimates provide decisionmakers with comparison baseline approximations for planning and budgeting annual costs. Absent life-cycle cost estimates for measuring and evaluating system costs and benefits, acquisitions become vulnerable because insufficient cost, schedule, and performance information exists to evaluate and justify investments for development, deployment, operations and maintenance.

Risk Management Plan. The Defense Intelligence Agency did not develop a DCIIS risk management plan to establish processes for identifying, assessing, and eliminating or reducing risks to acceptable levels. Although plans cannot identify all risks and accurately assess rates of occurrences and subsequent consequences, plans provide managers and decisionmakers with tools to forecast

costs, schedule development and deployment life-cycle events, and measure qualitative performance. Without risk management plans, managers and decisionmakers are unprepared to deal with complications and events that can affect the acquisition process.

Software Development Plan. The Defense Intelligence Agency did not document software develop plans for DCIIS. Software development plans outline and describe the development process for preliminary and critical design reviews, sub-system design reviews, data flow analysis, design and code walkthroughs, and interface reviews. Further, to avoid misunderstandings, user involvement is essential during reviews and analyses; however, documentation demonstrating that reviews, analyses, and walkthroughs occurred was not always evident. As a result, delays occurred and development costs increased because developers misinterpreted user requirements.

Development and Deployment

Development and deployment of DCIIS depended on the quality of MDITDS project management and delivered software products. When ASD(C3I) decided to combine the DCIIS acquisition with the MDITDS acquisition and use the MDITDS common database solution to store counterintelligence data, he assumed that the Defense Intelligence Agency could concurrently manage and oversee the DCIIS requirement for a new system and modernize the MDITDS legacy systems at the same time. The ASD(C3I) also assumed that the MDITDS common database would adequately serve the information system needs of DCIIS users.

Managing DCIIS and MDITDS. The Defense Intelligence Agency was not prepared to manage and oversee the DCIIS acquisition. It was a new start requiring a different acquisition strategy than the MDITDS. DCIIS was a high-risk system acquisition when compared to the MDITDS.

MDITDS. MDITDS was an evolving system. Prior automated information system solutions had been developed and deployed for the business processes. As a result of those prototypes, comparison benchmarks for requirement determinations and performance specifications existed for measuring system acquisition progress and results.

DCIIS. DCIIS was a new system start. Business processes for counterintelligence collections, investigations, operations, analysis and production and functional services were being automated for the first time. Users needed to be continually involved with product development to determine whether the project management office and system developers were building acceptable products for the information solution. As a result, program documentation needed to be established for translating system requirements to deliverable products, and baseline benchmarks needed to be determined for measuring the acquisition's cost, schedule, and performance effectiveness.

The Defense Intelligence Agency did not engage DCIIS users in the design of the system. Users were involved when developers demonstrated product functionality after system design and software coding. As a result, the

counterintelligence community of users did not have an opportunity to evaluate whether the selected DCIIS solution met the desired requirements and required system interfaces. Further, some software deliverables could not be traced to system requirements.

Also, the Defense Intelligence Agency was managing and overseeing an array of MDITDS and DCIIS contractual actions. At one time, 18 separate tasks existed for the combined acquisitions. As a result, when the Defense Intelligence Agency deployed Version 1.0 of MDITDS, the DCIIS module was not activated because it had not been fully developed.

Common Database Solution. The MDITDS common database solution was not suited for the DCIIS business processes. Before DCIIS tasking by ASD(C3I) in October 1995, the Defense Intelligence Agency reviewed 10 database applications for storing MDITDS information to determine whether the applications could functionally and technically meet legacy system requirements with a common database. In May 1995, the Defense Intelligence Agency selected the Memex® database for its text search ability and Internet adaptability.

However, the Memex® text search database was not entirely suited for the DCIIS business process, because DCIIS required an indexed relational database rather than one that enabled access to each character, word, punctuation mark, and symbol. As a result, DCIIS users required additional database queries because Memex® could not support the following functions:

- Structured Query Language searches without an external application that added time to return a result;
- Truncation or wild card searches that automatically extended root words;
- "More-like-this" searches to retrieve other documents that were similar to selected words; and
- Multiple Index searches that reduced numbers of documents and processing times.

Project Management and Program Oversight

Project management and program oversight for the MDITDS and DCIIS acquisitions were assigned and delegated to personnel with inadequate information technology training and experience. As a result, a disciplined acquisition approach for the development and deployment of the systems was not followed until the Defense Intelligence Agency functionally realigned project management and program oversight for information technology acquisitions with its Information Systems and Services/Systems Group and Chief Information Officer.[4]

[4]Program management responsibilities for the MDITDS and DCIIS acquisitions were the responsibility of the Directorate for Analysis and Production prior to the November 1999 realignment.

Project Management. In November 1999, the Information Systems and Services/Systems Group assigned a trained and experienced program manager to the MDITDS and DCIIS acquisitions. Assessing whether the systems were delivering acceptable deployed software products to its users, the program manager concluded after several months that both acquisitions were progressing without management controls for determining effectiveness and suitability. Specifically, the program manager found that:

- Acquisition documentation was not current,
- Software was not being developed in manageable increments,
- Development was not functionally prioritized,
- Software deliveries included functions that were not approved and that were degrading performance,
- Maintenance contracts were not in place for anticipated deployments, and
- Software deliveries passed integration tests but did not the meet the needs of users.

Program Oversight. Acquisition oversight did not exist for the MDITDS and DCIIS programs. Although several oversight boards existed, their primary responsibilities, as demonstrated by following descriptions, were not acquisition oversight.

- The Program Management Board coordinated requirements to ensure that the system acquisitions achieved functional objectives.
- The DoD Intelligence Information Systems Management Board ensured that the acquisitions complied with the information system management strategy for DoD intelligence.
- The Configuration Control Board was responsible for overseeing functional and physical characteristics of the systems' configuration and controlling, recording and reporting changes made to configured items.

Reacquiring DCIIS

In October 2000, the ASD(C3I) began planning for another counterintelligence system. However, unlike the previous acquisition, project management of the replacement system, also known as DCIIS, would remain within the Office of the ASD(C3I) and be assigned to the Director of Counterintelligence. Experienced system acquisition personnel at the program management office would manage the system development, deployment, operation, and maintenance. The Milestone Decision Authority for the designated Acquisition Category III program is expected to be assigned to the Defense Threat Reduction Agency, with functional oversight remaining with the ASD(C3I).

Since October 2000, the Director, Counterintelligence has assembled documentation and formed integrated product teams in support of a Milestone B (System Development and Demonstration) decision planned for FY 2002. A Mission Need Statement was not required because one was previously developed

and approved for the discontinued acquisition. An evaluation of database alternatives resulted in a recommendation to use a relational database management system for prototyping the first block of software for the replacement system's collection module. An Operation Requirements Document and a User Functional Description and Test Evaluation Management Plan were almost complete, and a functional requirement baseline was being developed. In addition, a software sub-system specification for the collections module had been completed and specifications for other modules were almost complete or were underway.

The Director formed five integrated product teams to address testing; training; information security; integration, interoperability, and architecture; and support and fielding. The Director also entered into an agreement with the Joint Interoperability Test Command to create a test bed for the DCIIS collections, investigations, operations, functional service, and analysis and production modules.

To comply with DoD guidance, DCIIS software development will evolve in four blocks. Further, the Counterintelligence Directorate planned to comply with Clinger-Cohen Act requirements by:

- Preparing cost benefit analyses throughout the life cycle of the system.
- Implementing performance measures to provide information for measuring program cost, schedule, and performance progress.
- Proceeding in a timely fashion toward agreed-upon life-cycle milestones, and
- Continually monitoring and evaluating the information technology investment for determining whether to continue, modify, or terminate the acquisition.

From FY 2002 through FY 2007, the ASD(C3I) will invest more than $45 million in the development, deployment, operation, and maintenance of the redefined DCIIS.

Conclusion

The ASD(C3I) and the Defense Intelligence Agency made the discontinued DCIIS a high-risk information technology investment because they did not apply management controls for cost-effectively acquiring, monitoring, testing, and preparing the DCIIS information technology acquisition for deployment and system life-cycle support in accordance with Office of Management and Budget and DoD guidance. Also, the ASD(C3I) decision to link DCIIS with the development and deployment of MDITDS and its database technology further stressed the system's development and user acceptance of anticipated software deployments. As a result, the ASD(C3I) ceased funding the Defense Intelligence Agency's acquisition of DCIIS due to delays and user dissatisfaction with delivered software products and was reacquiring the automated information system using a disciplined acquisition strategy within his counterintelligence directorate.

Recommendations and Management Comments

We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), in implementing a disciplined acquisition strategy for the reacquired Defense Counterintelligence Information System:

1. Establish management controls for translating mission needs into a set of operational requirements.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred. A Mission Needs Statement has been developed and an Operational Requirements Document is in final coordination. The Director of Counterintelligence's complete text of the comments is in the Management Comments section.

2. Create a structured, integrated system life-cycle plan with cost, schedule, and performance goals for measuring progress and projecting results.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred. A system life-cycle plan has been established for tracking and monitoring program progress. The Director of Counterintelligence's complete text of comments is in the Management Comments section.

3. Maintain documentation for continually justifying the selected solution as the best of alternatives.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred. Weekly assessments are being made to assure that the selected solution is the best alternative. The Director of Counterintelligence's complete text of comments is in the Management Comments section.

4. Perform continual assessments of acquisition and security risks with planned actions taken to mitigate them.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred. A Risk Management Plan is being developed, and program security is being continually reviewed. The Director of Counterintelligence's complete text of comments is in the Management Comments section.

5. Allocate program development and deployment risks between the Government and contractors.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred. Management processes are being established to balance development and deployment risks. The Director of Counterintelligence's complete text of comments is in the Management Comments section.

6. Maximize use of commercial technology and competition.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred. Commercial technology is being used for prototyping the initial module, and technical advisors are providing information to increase program effectiveness that includes available technology and competition. The Director of Counterintelligence's complete text of comments is in the Management Comments section.

7. **Prepare and submit quarterly acquisition oversight reports to functional and acquisition Milestone Decision Authorities.**

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred. The reacquired information technology system has been designated as an Acquisition Category III program and will provide quarterly oversight reports to the Senior Counterintelligence Functional Manager and the Milestone Decision Authority. The Director of Counterintelligence's complete text of comments is in the Management Comments section.

Appendix A. Audit Process

Scope

Work Performed. We reviewed documentation dated from June 1995 through October 2001. To accomplish the audit objective, we:

- Interviewed officials and obtained documentation from the ASD(C3I) Counterintelligence Division, the Defense Intelligence Agency MDITDS Program Management Office, cognizant officials and personnel involved in the acquisition of the DCIIS information technology investment, and contractor personnel.
- Reviewed available documents related to program requirements, program definition, program assessments and decision reviews, periodic program status reporting, program management and oversight, and information system security.
- Evaluated the adequacy of management controls related to the acquisition of DCIIS information technology investment.

General Accounting Office High-Risk Area. The General Accounting Office identified several high-risk areas in the DoD. This report provides coverage of the DoD Systems Modernization high-risk area.

Methodology

Audit Type, Dates, and Standards. We conducted this program audit from March 2001 through November 2001 in accordance with generally accepted Government auditing standards. We did not use computer-processed information to perform this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provide reasonable assurance that programs are operating as intended and to evaluate the adequacy of those controls.

Scope of the Review of the Management Control Program. In accordance with DoD Directive 5000.1, DoD Instruction 5000.2, "Operation of the Defense Acquisition System," October 23, 2000, and DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," March 15, 1996 (subsequently revised on January 4, 2001), acquisition managers are to apply program cost, schedule, and performance parameters to control objectives for implementing DoD Directive 5010.38 requirements. Accordingly, we limited our review to management controls directly related to the acquisition management of the DCIIS. We also reviewed management's self-evaluation of management controls applicable to the acquisition of DCIIS information technology.

Adequacy of the Management Controls. Before the ASD(C3I) reacquisition of the replacement DCIIS in FY 2001, management controls were inadequate for the information technology acquisition. System life-cycle plans and program baselines were not developed for the information technology investment. As a result, an internal management control system for monitoring program performance and progress could not be implemented. Cost, schedule, and performance deviations could not be identified, and measurement indices could not be computed for projecting results. The actions being taken by ASD(C3I) to follow a disciplined acquisition strategy for the replacement DCIIS, in conjunction with our recommendation for tracing product requirements to software deliverables, managing risks, and preparing reports for oversight assessments, can help avoid the material management control weaknesses associated with the discontinued acquisition. A copy of the report will be sent to the senior official in charge of management controls for the ASD(C3I).

Adequacy of Management's Self-Evaluation. Neither the ASD(C3I) nor the Defense Intelligence Agency identified DCIIS as an assessable unit.

Prior Coverage

During the last 5 years, no reports addressing the DCIIS information technology investment were issued.

Appendix B. Acquisition Guidance

The Office of Management and Budget and DoD provide managers with guidance for acquiring information technology investments and safeguarding information assets.

Office of Management and Budget

Office of Management and Budget Circular No. A-123, "Management Accountability and Control," June 21, 1995, issued under the authority of the Federal Managers' Financial Integrity Act of 1982, provides guidance regarding management accountability and controls for establishing management controls, assessing and improving management controls, correcting management control deficiencies, and reporting on management controls. The Circular references Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," November 30, 2000, as a source for evaluating whether systems and applications are:

- achieving their intended results,
- using resources consistent with the agency's mission,
- protecting programs and resources from waste, fraud, and mismanagement,
- following laws and regulations, and
- obtaining, maintaining, reporting and using reliable and timely information for decisionmaking.

Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," November 30, 2000, implements numerous public laws and other Office of Management and Budget guidance that address the acquisition of information technology investments and the security of personal information. In accordance with the Clinger-Cohen Act of 1996, the Circular requires that:

- Cost benefit analyses be prepared for each system throughout its life cycle.
- Performance measures be implemented to provide timely information on the progress of an information technology program in terms of cost and capability to meet specified requirements, timeliness, and quality.
- Major information systems proceed in a timely fashion toward agreed-upon milestones in an information system's life cycle.
- Chief information officers monitor and evaluate the performance of information technology investments through the capital planning investment control process, and advise the agency head on whether to continue, modify, or terminate a program or project.

Further, Circular A-130 requires management controls for safeguarding information assets. Those controls include:

- security plans for all systems containing sensitive information,
- periodic security reviews to determine the effectiveness of controls, and
- a security control assessment by a management official before a system processes information.

DoD Guidance

DoD Directive 5000.1. DoD Directive 5000.1, "Defense Acquisition," March 15, 1996 (subsequently revised on October 23, 2000), establishes a disciplined, life-cycle management approach for acquiring quality products. DoD Directive 5000.1 requires rigorous internal management control systems for identifying deviations from approved program baselines.

DoD Directive 5200.28. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, provides mandatory guidance for safeguarding classified information and information that might affect the privacy of DoD personnel. It implements security safeguard provisions of Office of Management and Budget Circular A-130. It is also a reference source for DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," June 1, 1998.

DoD Directive 8000.1. DoD Directive 8000.1. "Defense Information Management (IM) Program," October 27, 1992, establishes policy and assigns responsibilities for the collection, creation, use, dissemination, and disposition of all data and information within DoD. In addition, DoD Directive 8000.1 defines information security, integrity and survivability as basic to DoD missions. Also, the Directive requires a disciplined life-cycle approach to manage information systems.

DoD Instruction 5000.2. DoD Instruction 5000.2, "Operation of the Defense Acquisition System," Change 1, January 4, 2001, establishes a general approach for managing system acquisitions with best life-cycle solutions for satisfying user requirements. DoD Instruction 5000.2 requires chief information officers to confirm that mission-critical and -essential information systems are developed in accordance with the Clinger-Cohen Act of 1996 before approvals are granted for milestone advancements.

DoD Regulation 5000.2-R. DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," June 2001, establishes life-cycle procedures for managing major acquisition programs and a model for other system acquisitions.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Director, Administration and Management

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Intelligence Agency
  Inspector General, Defense Intelligence Agency
Director, National Security Agency
  Inspector General, National Security Agency

Non-Defense Federal Organizations

Office of Management and Budget
  Office of Information and Regulatory Affairs

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform
House Permanent Select Committee on Intelligence

This page was left out of original document

Assistant Secretary Of Defense (Command, Control, Communications, And Intelligence) Comments

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

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

7 January, 2002

Memorandum For: Office of the Department of Defense Inspector General (attn: Ms Ugone).

Subject: DoD Inspector General memorandum subject; Audit Report on the Acquisition Management of the Defense Counterintelligence Information System (Project No. D2001AL-0073) November 9, 2001.

The following comments are provided in response to Subject report (attached):

DoD IG Finding; "The ASD (C3I) and the Director, Defense Intelligence Agency, had made the discontinued DCIIS a high risk information technology investment because they:"

- "did not implement project management controls and oversight for cost-effectively, monitoring, testing, and preparing the information technology acquisition for deployment and system life-cycle support in compliance with Office of Management and Budget and DoD guidance, "
- "linked the DCIIS development and deployment to the MDITDS and its database technology."

Concur. The ASD (C3I) closely monitored program progress, associated costs and support. The DIA Director maintained a Program Management Board (PMB) with sub-panels in order to address program issues. The ASD (C3I) arranged for operational test planning and support directly with the DoD Office of Operational Test and Evaluation (OT&E) for DCIIS. However, the ASD (C3I) placed reliance for DCIIS acquisition management, software development, software contracting and Data Base Management System (DBMS) selection with the DIA-MDITDS Program Office. The DBMS technology selected by the MDITDS Program Office subsequently proved incapable of supporting DCIIS program goals. As a result, during January 2001, steps were taken to provide 100% oversight of the DCIIS effort by establishing the DCIIS Program Management Office (PMO) within the ASD (C3I). This was done as a result of lessons learned from the previous effort where over reliance had been placed on another agency.

DoD IG Finding. "As a result, the Director Counterintelligence, Office of Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is reacquiring the DCIIS, because a business need still exists for a joint information system that gathers and reports counterintelligence data. Further the Director intends to follow a disciplined acquisition strategy for system life-cycle development, deployment, operation, and maintenance by avoiding and reducing risks that caused deployment delays and user dissatisfaction with the prior DCIIS acquisition."

Concur. New DCIIS program management and development efforts are in full compliance with the DoD 5000 series acquisition instructions. The new DCIIS effort has been designated as an Acquisition Category (ACAT) III level program in coordination with the Office of the Chairman of the Joint Chiefs of Staff (J-8). The new DCIIS Program Office is working diligently to create all of the acquisition documentation required to support a Milestone B decision to be made by the DoD Deputy Chief Information Officer (DCIO) planned for January 2002. Recent demonstrations of the first DCIIS module have met with high praise from users. The first DCIIS module is expected will be tested and fielded during the early months of calendar year 2002. During the time period the previous DCIIS program was under development considerable knowledge was gained by the CI community, DIA and the MDITDS Program Office to address what DCIIS should be. As a result of the efforts of several members of the counterintelligence community, DIA and the MDITDS Program Office the new DCIIS program will produce a successful outcome far sooner than would have been the case if this previous foundation work had not been accomplished.

DoD IG Recommendations:
1. Establish management controls for translating mission needs into a set of operational requirements.

Concur. The new DCIIS program is designated as an ACAT III acquisition program. The new DCIIS program is fully implementing DoD 5000 acquisition ACAT III level management instructions. A Mission Needs (MNS) Statement has been developed and approved. An Operational Requirements Document (ORD) is in for final coordination with the CI community leadership and the Joint Forces Command.

2. Create a structured, integrated system life-cycle plan with cost, schedule and performance goals for measuring progress and projecting results.

Concur. The new DCIIS Program has established a PM reporting system to insure all life-cycle plan milestones; cost elements and performance goals are monitored to insure program progress is effectively and realistically tracked.

3. Maintain documentation for continually justifying the selected solution as the best of alternatives

Concur. The new DCIIS program conducted an intensive analysis of alternatives (AOA) effort to identify the best solution to meet mission needs. The AOA effort was fully documented. Weekly assessments are made by the Defense Counterintelligence Requirements Panel (DCIRP) to insure the selected solution is the best of the alternatives examined.

4. Perform continual assessments of acquisition and security risks between Government and contractors.

Concur. Ongoing assessments are made by the DCIIS PM and staff to insure both acquisition and security risks between Government and contractors are addressed on a

continuing basis. The DCIIS PM is developing a Risk Management Plan and instituting use of Risk Management Tools as part of DCIIS program management. Continual review of program security is being accomplished under the DCIIS PM's direction through the Information Systems Security (INFOSEC) Integrated Process Team (IPT).

5. Allocate program development and deployment risks between the Government and contractors.

Concur. The DCIIS PM has established management processes to insure proper balance is maintained between development and deployment risks. Management processes are accomplished through assessments made by the DCIIS PM and staff to insure requirement's clarity, schedule completion and costs are both detailed and accounted for.

6. Maximize use of commercial technology and competition.

Concur. Commercial technology is being used to prototype the initial DCIIS module. An analysis of alternatives was completed to identify commercial products and firm's best suited to provide the best technical solution. In addition, the DCIIS PM has technical advisors on staff to monitor and assess current and emerging technology to recommend/provide best application of technology to the problem set. These technical advisors provide supporting information concerning methods to maximize program effectiveness which includes appropriate use of resources, direct application of readily available technology products, unique expertise, and competition.

7. Prepare and submit quarterly acquisition oversight reports to functional and acquisition Milestone Decision Authorities.

Concur. The DCIIS program has been established as ACAT III. The DoD Deputy Chief Information Officer (DCIO) will act as the temporary Milestone Decision Authority until the newly established Counterintelligence Field Activity (CIFA) designates a Chief Information Officer (CIO). Throughout all DCIIS development phases the program will provide continuous quarterly acquisition oversight reports to the Senior Counterintelligence Functional Manager and the DCIIS Milestone Decision Authority.

David A. Burtt, II
Director
Counterintelligence

ODASD OR&M 1/8/01
Investment and Acquisition
(Coordination)

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Mary Ugone
Charles M. Santoni
David M. Wyte
Walter S. Bohinski
Donald Stockton
Jenshel D. Marshall
Jacqueline N. Pugh