~~FOR OFFICIAL USE ONLY~~

Audit Report

YEAR 2000 CONVERSION PROGRAMS OF THE
DEFENSE INTELLIGENCE AGENCY

Report No. 99-098 March 4, 1999

Office of the Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~

Additional Copies

To obtain additional copies of this audit report, 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 or visit the Inspector General, DoD, Home Page at: WWW.DOGIG.OSD.MIL

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Audit Followup and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) 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, Virginia 22202-2884

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, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DAWN	Defense Attaché Worldwide Network
DIA	Defense Intelligence Agency
HOCNET	Human Intelligence Operational Communications Network
JWICS	Joint Worldwide Intelligence Communications Systems
MDITDS	Migration Defense Intelligence Threat Data System

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

March 4, 1999

MEMORANDUM FOR DIRECTOR, DEFENSE INTELLIGENCE AGENCY

SUBJECT: Audit Report on Year 2000 Conversion Programs of the Defense Intelligence Agency (Report No. 99-098)

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

Management comments conformed to the requirements of DoD Directive 7650.3.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to [redacted] at (703) 604-[redacted] (DSN 664-[redacted]) e-mail <[redacted]@dodig.osd.mil>, or [redacted] at (703) 604-[redacted] (DSN 664-[redacted]) e-mail <[redacted]@dodig.osd.mil>. See Appendix D for the report distribution. The audit team members are listed on the inside back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-098 **March 4, 1999**
(Project No. 8AS-0032.08)

Year 2000 Conversion Programs of the Defense Intelligence Agency

Executive Summary

Introduction. This report is one in a series issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor efforts to address the year 2000 computing challenge. For a listing of audit projects addressing the issue, see the year 2000 webpage on the Inspector General internet at http://www.ignet.gov.

Audit Objectives. Our objective was to determine whether planning and management were adequate to ensure that year 2000-related issues would not unduly disrupt continuity of operations at the Defense Intelligence Agency. Specifically, we reviewed actions taken by the Defense Intelligence Agency to resolve date-processing issues relating to the year 2000, as well as preparation of plans to address year 2000-related system failures that could affect the ability of the Defense Intelligence Agency to perform its mission.

Audit Results. We reviewed 11 mission-critical systems for the Defense Intelligence Agency and 8 high-impact systems managed by other DoD organizations. The Defense Intelligence Agency reported that 2 of the 11 mission-critical systems would not be year 2000 compliant by December 31, 1998. However, contingency plans had been prepared or were in process for all 11 systems. In addition, the Defense Intelligence Agency made significant progress in developing facility contingency plans and prioritizing, replacing, and repairing infrastructure systems. However, the Defense Intelligence Agency had not planned a security reaccreditation review of mission-critical systems that had undergone major renovation. In addition, the Defense Intelligence Agency had not developed work-around strategies for three of eight high-impact systems, managed by other organizations, that were not year 2000 compliant by December 31, 1998. Also, the Defense Intelligence Agency had not provided sufficient system information to unified command users to aid them in developing effective contingency plans for their organizations. See Part I for details.

Summary of Recommendations. We recommend that the Defense Intelligence Agency determine whether mission-critical systems that had major renovations need a security reaccreditation review. We also recommend that the Defense Intelligence Agency develop and include work-around strategies for noncompliant, high-impact

systems, which are managed by other DoD organizations, in its operational contingency plan. We further recommend that the Defense Intelligence Agency provide contingency plans for its information systems to unified command users.

Management Comments. The acting director, Defense Intelligence Agency, concurred with all recommendations and stated that the Chief Information Security Officer, Defense Intelligence Agency, had reviewed changes to all its mission-critical systems; the Defense Intelligence Agency operational contingency plans will be ready by the DoD deadline of March 31, 1999, and will include work-around strategies for high-impact systems managed by other DoD organizations; and the Defense Intelligence Agency will provide system technical contingency plans to all appropriate users. Part I of this audit report discusses management comments. Part III of the report provides the complete text of management comments.

Table of Contents

Part I - Audit Results

Audit Background

Year 2000 Problem. Because of the potential failure of computers to run or function throughout the Government, the President issued Executive Order, "Year 2000 Conversion," February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program experiences disruption because of the year 2000 problem and that the head of each agency ensure that efforts to address the year 2000 problem receive the highest priority attention in the agency.

DoD Year 2000 Management Strategy. The "DoD Year 2000 Management Plan" describes a five-phase year 2000 management process, which includes awareness, assessment, renovation, validation, and implementation phases. Although the Office of the Assistant Secretary of Defense (Command, Control, Communication and Intelligence) issued draft versions of the DoD Year 2000 Management Plan, DoD intended Defense Components to accomplish the phases within the target dates shown in the document. The three drafts and final version established December 31, 1998, as the target date for deploying renovated mission-critical systems and completing contingency plans for those systems.

Defense Intelligence Agency Year 2000 Management Strategy. The "DIA [Defense Intelligence Agency] Year 2000 Strategic Plan," April 7, 1998, uses the five-phase approach that DoD applied and added a sixth phase of compliance assurance. DIA added the compliance assurance phase in anticipation of the need to repair, renovate, and monitor systems after the completion of the formal year 2000 efforts. The strategic plan states that, historically, new software development efforts have not met on-time delivery schedules; therefore, prudence dictates a need for a migration system contingency plan if implementation is delayed.

DIA established the DIA Year 2000 Project Management Office to manage and to serve as the focal point for its year 2000 effort. The DIA Year 2000 Project Management Office is responsible for establishing agency-wide strategies and policy guidance for addressing the year 2000 problem, providing technical assistance to the directorates, overseeing the progress of all year 2000 remedial efforts, ensuring that contingency plans for all mission-critical systems are developed and updated on a regular basis, and for maintaining a central file of signed compliance certificates. The DIA directorates are responsible for developing and implementing detailed year 2000 milestones, strategies, and test plans for systems within their functional areas; assessing and validating systems and system interfaces for year 2000 compliance; and repairing, retiring, or replacing noncompliant systems.

Audit Objectives

The audit objective was to determine whether planning and management are adequate to ensure that year 2000-related issues would not unduly disrupt continuity of operations at the Defense Intelligence Agency. Specifically, we reviewed actions taken by DIA to resolve date-processing issues relating to the year 2000, as well as preparation of plans to address year 2000-related system failures that could affect the ability of DIA to perform its mission. We did not review the management control program related to the overall audit objective, because DoD recognized the year 2000 issue as a material management control weakness area in the FY 1997 and FY 1998 Annual Statements of Assurance. See Appendix A for a discussion of the scope, methodology, and summary of prior coverage.

Status of Defense Intelligence Agency Mission-Critical Systems for Year 2000

DIA recognized the importance of the year 2000 issue and took action to address year 2000 problems within DIA. DIA established the Year 2000 Project Management Office to provide oversight of year 2000 remedial efforts, to monitor development of contingency plans, and to coordinate year 2000 reporting. However, DIA system project managers had not requested security reaccreditation reviews for mission-critical systems that had major renovations, because they did not believe reaccreditation was necessary. DIA had not included work-around strategies in its operational contingency plan for high impact systems managed by other Defense organizations, because DIA lacked procedures requiring those strategies. In addition, DIA had not provided sufficient information for its systems to unified command users, because the DIA Year 2000 Project Management Office was under time constraints and focused on internal DIA year 2000 efforts. Not performing security reviews of systems increases risk of intrusions into the systems renovated. In addition, not developing work-around strategies for high impact systems external to DIA and not providing contingency plans of DIA systems to unified command users could increase the likelihood of year 2000 system disruptions within DIA and the unified commands.

Actions Taken to Address the Year 2000 Problem

The Year 2000 Project Management Office disseminated guidance, provided technical assistance to project offices, reviewed project office year 2000 efforts, coordinated mission-critical system reporting, and oversaw the development of contingency plans for mission-critical systems. The DIA Year 2000 Program Office provided the following assistance:

- developed the "DIA Year 2000 Strategic Plan";
- established a year 2000 working group;
- established a year 2000 home page to post year 2000-related information;
- contacted current vendors to determine actions to ensure year 2000 compliance;
- held monthly and quarterly meetings to update DIA senior management on the status of year 2000 efforts;
- attended DoD year 2000 working group and interface assessment workshops; and

- attended intelligence community year 2000 working group meetings on testing, risk management and contingency planning, facilities, communication, and communication security.

Defense Intelligence Agency Mission-Critical Systems

Security Reaccreditation Review. System project managers did not request security reaccreditation reviews for mission-critical systems that had major renovations. DoD Directive, "Security Requirements for Automated Information Systems (AISs), March 21, 1988, states that any changes to the automated information system or associated environment that affect the accredited safeguards or result in changes to the prescribed security requirements shall require reaccreditation. Reaccreditation shall take place before the revised system is declared operational. The directive states that, minimally, an automated information system shall be reaccredited every 3 years, regardless of changes.

Of the 11 DIA mission-critical systems reviewed, 3 systems required changes to lines of coding to resolve year 2000 date-processing issues. The project managers for the Communications and Message Profiler, the High Performance Computer System, and the Support for the Analyst File Environment did not request security reaccreditation reviews to ensure that the coding changes did not affect the information security controls for software applications and operating systems. DIA: (b) (3), 10 USC § 424

[redacted]

Operational Contingency Plan

As of December 1998, DIA was still developing its operational contingency plan. The DoD Year 2000 Management Plan established March 31, 1999, as the target date that Defense Components should complete their operational contingency plans. The DoD Year 2000 Management Plan states that the group responsible for executing the core mission process should develop and execute the operational contingency plans. Planning includes developing and implementing work-around procedures necessary to execute the mission or to function at or above the minimum acceptable levels of functionality. The DoD Year 2000 Management Plan provides the following list to illustrate the content of a typical year 2000 operational continuity plan:

- Core business or organizational functions;
- Automated information systems to support the core functions;
- Emergency notification procedures with points of contact and phone numbers to report loss or degradation of supporting system functionality;
- Procedures for users of automated information systems to detect possible corrupt system data;
- Procedures for users to report a system fault to the maintainers or developers;

- Procedures to execute the functions of the failed system or infrastructure without the assistance of the automated information systems normally supporting that mission or function;
- Alternate suppliers for mission-critical supplies that may be unavailable or mission-limiting according to the worst-case scenario;
- Impact of the loss of automated information system functionality upon the organization or mission;
- Procedures to restore data collected by alternate means into the corrected or restored system(s); and
- Links to relevant system contingency plans, other operational contingency plans, and continuity of operations plans.

Facilities and Infrastructure Groups. As part of its effort to develop an operational contingency plan, DIA established two separate groups to review year 2000 issues relating to DIA facilities and information systems infrastructure. The facilities group developed a contingency plan to maintain limited operating capability should a disruption in utility services occur. DIA has scheduled a rehearsal of the back-up plan for July 1999. The information systems infrastructure group inventoried all stand-alone, personal, and laptop computers; prioritized the systems; and monitored the replacement or repair of the systems.

Externally Managed High Impact Systems. DIA did not include work-around strategies for three high-impact systems that were managed by other organizations in its operational contingency plan. In August 1998, DIA personnel identified the systems listed in Appendix C as critical mission-support systems. Because the managing DoD Components also identified the eight systems as mission critical to their organizations, they were required by the DoD Year 2000 Management Plan to fully implement the systems and to have completed system contingency plans by December 31, 1998. Although it received some information on the systems, the DIA Year 2000 Project Management Office officials did not believe that the implementation dates provided by the organizations were realistic. Of eight systems, five were not year 2000 compliant by December 31, 1998; and six systems had or were developing contingency plans. After the audit team provided information on the systems to the Year 2000 Project Management Office, DIA officials indicated that DIA would take action to avoid disruptions of DIA functions due to year 2000 failure of the high impact systems. Subsequent to the issuance of the draft of this report, the DIA officials reclassified one of the eight systems as non-mission critical to DIA and determined that DIA needed to develop work-around strategies for three of the remaining seven systems. The three systems are the Human Resources Management System, the Joint Collection Management Tool, and the National Exploitation System.

System Contingency Plans to Unified Command Users

Officials in the DIA project management office noted that DoD did not require contingency plans be in place prior to December 31, 1998. DIA will establish a homepage and put its systems' contingency plans on Intelink.

Conclusion

DIA had made significant progress in addressing year 2000 issues. Of 11 mission-critical systems, 10 systems had adequate contingency plans and the remaining system's plan was in draft. Nine mission-critical systems were reported year 2000 compliant as of December 31, 1998. DIA appropriately reported two systems to DoD and the Office of Management and Budget as late. Because several of DIA mission-critical systems were renovated, DIA needs to determine whether the systems require a security reaccreditation review. DIA is developing an operational contingency plan to minimize disruptions due to year 2000 problems; however, DIA did not include work-around strategies for externally managed high impact systems that will not be compliant. In addition, DIA should provide contingency plans of its systems to the unified commands to help them develop effective operational contingency plans for their own organizations. Implementation of the following recommendations should ensure the security of DIA mission-critical systems and also reduce the likelihood of year 2000 system disruptions within DIA and within organizations that use DIA systems.

Recommendations and Management Comments

We recommend that the Director, Defense Intelligence Agency:

1. Task the Chief Information Security Officer, Defense Intelligence Agency, to review all mission-critical systems that had major renovations to determine whether they require a security reaccreditation review;

2. Develop and include work-around strategies in its operational contingency plan for high impact systems managed by other Defense organizations; and

3. Provide contingency plans for its information systems to its unified command users.

DIA Comments. Responding for the Director, Defense Intelligence Agency, the acting director concurred with Recommendations 1., 2., and 3., stating that the Chief Information Security Officer, Defense Intelligence Agency, had reviewed changes to all its mission critical systems; the Defense Intelligence Agency operational contingency plans will be ready by the DoD deadline of March 31, 1999, and will include work-around strategies for high impact systems managed by other Defense organizations; and the Defense Intelligence Agency will provide system technical contingency plans to all appropriate users.

Part II - Additional Information

Appendix A. Audit Process

This report is one in a series that the Inspector General, DoD, issued in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor efforts to address the year 2000 computing challenge. For a listing of audit projects addressing this issue, see the year 2000 webpage on Inspector General internet at <http://www.ignet.gov>.

Scope

Work Performed. We reviewed actions taken by DIA to resolve date-processing issues for the year 2000 for 11 mission-critical systems. In addition, we reviewed system implementation schedules, test plans, and contingency plans to address year 2000-related system failures that could impact the ability of DIA to perform its mission. We also reviewed briefing charts provided to DIA senior managers and reports to DoD on the status of DIA mission-critical systems. We based our review on DoD and DIA year 2000 guidance.

DoD-wide Corporate Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Department of Defense established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting those objectives. This report pertains to achievement of the following objectives and goals:

- **Objective:** Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. **(DoD-3)**

- **Objective:** Fundamentally reengineer DoD and achieve a 21st century infrastructure. **Goal:** Reduce costs while maintaining required military capabilities across all DoD mission areas. **(DoD-6)**

DoD Functional Areas Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievements of the following functional area objectives and goals in the Information Technology Management Functional Area:

- **Objective:** Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM 1.2)**

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate DoD information infrastructure. **(ITM 2.2)**

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Upgrade technology base. **(ITM 2.3)**

- **Objective:** Ensure that vital information on DoD resources are secure and protected. **Goal:** Assess information assurance posture of DoD operational systems. **(ITM 4.4)**

General Accounting Office High-Risk Area. The General Accounting Office identified several high-risk areas in DoD. This report provides coverage of the Defense Information Management and Technology high-risk areas.

Methodology

Audit Methodology. To evaluate DIA efforts to achieve year 2000 compliance, we reviewed all DIA mission-critical systems, and the eight high impact systems not managed by DIA. For each system reviewed, we:

- determined whether DIA and other Defense organizations had primary responsibility for ensuring that the system would be year 2000 compliant;
- determined whether DIA or other Defense organizations had scheduled the full implementation of a year 2000 compliant system;
- determined whether the noncompliant systems were properly reported as late to DoD and the Office of Management and Budget; and
- reviewed the adequacy of the contingency plans for each system.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Audit Period, Standards, and Locations. We conducted this program results audit from August 1998 through December 1998, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

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

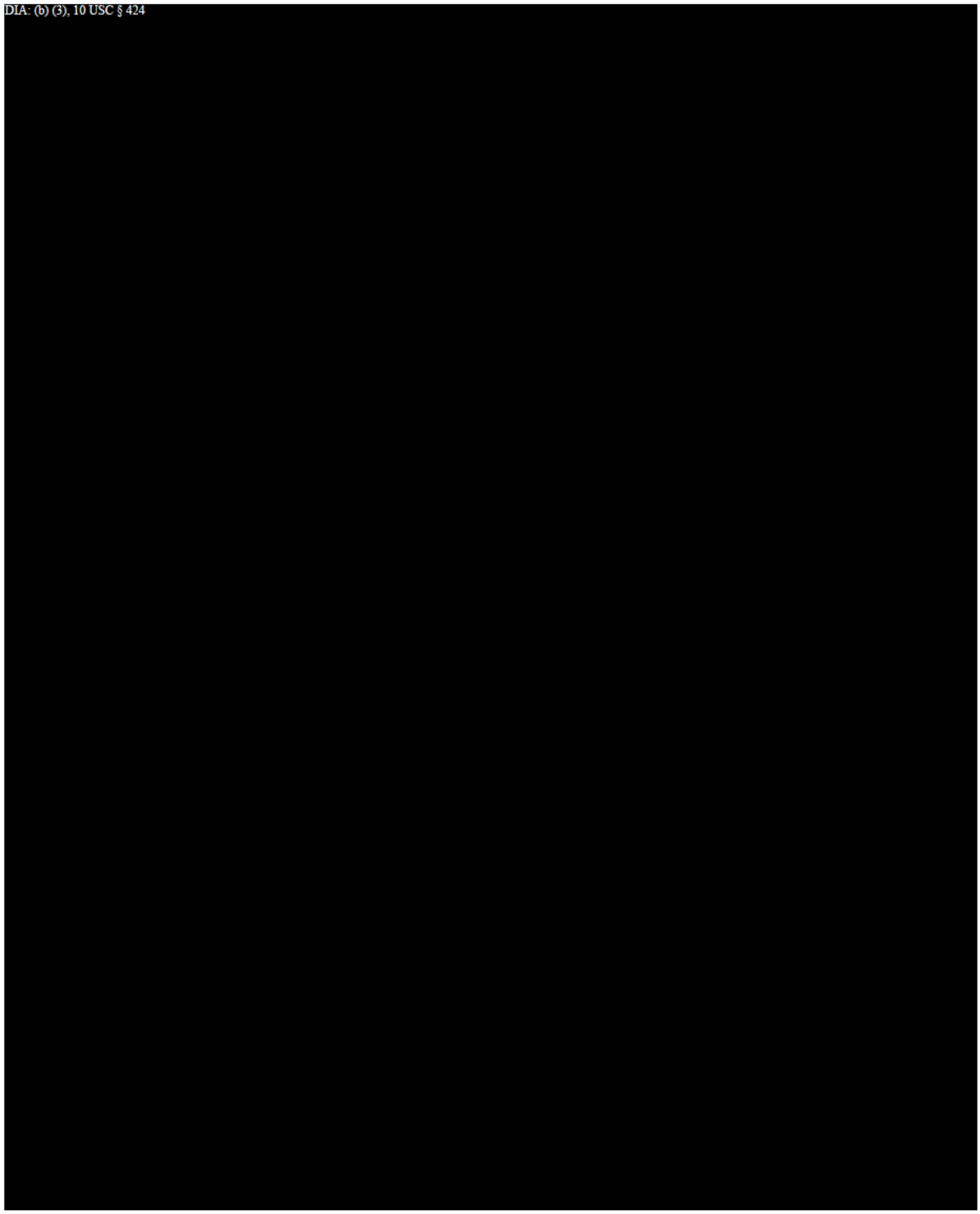
Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the year 2000 issue as a material management control weakness area in the FY 1997 and FY 1998 Annual Statements of Assurance.

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to year 2000 issues. General Accounting Office reports can be accessed over the internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed over the internet at http://www.dodig.osd.mil.

Appendix B. Defense Intelligence Agency Mission-Critical Systems

DIA: (b) (3), 10 USC § 424



Appendix C. High Impact Systems Not Managed By Defense Intelligence Agency

System	System Owner	Full Implementation Date	Contingency Plan	Status[1]
Communications Support Processor (CSP)	Air Force	December 1999	None	Late
Defense Civilian Payroll System (DCPS)	NSA[2]	September 1998	Being Developed	
Defense Message System (DMS)	DISA[3]	December 1999[4]	Adequate	Late
Human Resources Management System (HRMS)	NSA	May 1999	Being Developed	Late
Joint Collection Management Tool (JCMT)	Army	May 1999	Being Developed	Late
Joint Targeting Toolbox (JTT)[5]	Air Force	May 1999	Being Developed	Late
National Exploitation System (NES)	NIMA[6]	July 1999	Being Developed	Late
Requirements Management System (RMS)	NIMA	February 1999	None	Late

[1]Implementing date is after December 31, 1998. As of September 1998, only the Requirements Management System was reported as late to the Office of Management and Budget.

[2]National Security Agency

[3]Defense Information Systems Agency

[4]The Defense Message System may not be available to replace some critical Automated Digital Network messaging capabilities by December 31, 1999, when the Automated Digital Network contract expires.

[5]Subsequent to the issuance of the draft report, DIA reclassified this system as non-mission critical and, therefore, no longer considers it a high impact system.

[6]National Imagery and Mapping Agency

Appendix D. 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)
  Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence, Surveillance, Reconnaissance, and Space Systems)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
    Principal Deputy-Y2K
Assistant Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief Information Officer, Department of the Army
Inspector General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
Chief Information Officer, Department of the Navy
Inspector General, Department of the Navy
Inspector General, Marine Corps
Superintendent, Naval Postgraduate School

Department of the Air Force

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

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Director, Defense Intelligence Agency
  Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office
Defense System Management College

Non-Defense Federal Organizations and Individuals

Chief Information Officer, General Services Administration
Office of Management and Budget
  National Security Division, Special Projects Branch
Technical Information Center, National Security and International Affairs Division, General Accounting Office
Director, Defense Information and Financial Management Systems, Accounting and Information Management Division, General Accounting Office

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

Senate Special Committee on the Year 2000 Technology Problem
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 National Security, Committee on Appropriations
House Committee on Government Reform and Oversight
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
House Committee on National Security
House Permanent Select Committee on Intelligence

Part III - Management Comments

Defense Intelligence Agency Comments

~~FOR OFFICIAL USE ONLY~~

DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D C. 20340-

FOUO-6,010 DIA: (b) (3), 10 USC Y2K 10 February 1999

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Draft Audit Report on Year 2000 Conversion Programs within the Defense Intelligence Agency (Project No. 8AS-0032.08)

1. At the Department of Defense Year 2000 (Y2K) Steering Committee meeting on 9 January 1999, DIA reported that 9 of our 11 mission-critical systems were Y2K compliant. Of the other two systems, one is well into its fielding schedule and the other is ready for final testing. DIA's current Y2K status is on track with our plan that was briefed to the DoD IG on 21 August 1998.

2 We have reviewed the draft audit report, concur with the comments, and have taken appropriate actions. The status of each recommendation is provided below.

a Recommendation: Task the Chief Information Security Officer, DIA, to review all mission-critical systems that had major renovations to determine whether they require a security review.

DIA Comments: Concur with comments. The Chief Information Security Officer, DIA, has reviewed changes to all DIA mission-critical systems. Information system security concerns are managed through the formal DIA change management process in accordance with Agency regulation DIAR 50-23, DIA Information System Security Management. Consistent with policy and procedures, the Chief Information Security Officer reviews all systems prior to initial fielding or upgrade. Additionally, the DIA mission-critical systems are tracked as part of the Director's metrics and have been reported to have no outstanding issues. DIA Y2K activities have never had a negative impact on the security of DIA automated information systems.

b. Recommendation: Develop and include work-around strategies in DIA's operational contingency plan for high-impact systems managed by other defense organizations.

DIA Comments: Concur with comments. DIA's long-standing approach has been to include these systems under the DIA Operational (Mission/Functional) Contingency Plans (CPs) vice the systems (Technical) CPs. DIA will have the Operational CPs ready by the the DoD deadline of 31 March 1999. The use of the term "high-impact" does not necessarily imply that the systems support an agency-critical function or mission.

c. Recommendation: Provide contingency plans for DIA information systems to Unified Command users.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

DIA Comments: Concur. System (Technical) CPs were developed for all DIA mission-critical systems by the DoD deadline of 30 December 1998. DIA system CPs will be provided to all appropriate users.

3 DIA requests that the final audit report be marked "For Official Use Only."

4. The point of contact is DIA: (b) (3), 10 USC § 424 DIA Y2K DIA: (b) (3), 10 USC § 424

JEREMY C. CLARK
Acting Director

~~FOR OFFICIAL USE ONLY~~

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.