DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-

30 September 2004

U-157/FE2

MEMORANDUM FOR THE SECRETARY OF DEFENSE

Thru: for UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Subject: Annual Statement Required for Fiscal Year 2004 under the Federal Managers' Financial Integrity Act (FMFIA) of 1982

1. As the Director of the Defense Intelligence Agency (DIA), I understand the importance of management controls. I have taken the necessary steps to ensure a conscientious and thorough evaluation of the management control program for the agency. Our evaluation enables me to provide reasonable assurance, with the noted exception, that DIA's management controls, taken as a whole, were in place, operated effectively and were being used during the fiscal year (FY) ending 30 September 2004. Our controls provided reasonable assurance that we achieved four FMFIA objectives by ensuring obligations and costs complied with law; safeguarding assets from fraud, waste, abuse and mismanagement; achieving intended program results; and using resources consistent with the agency mission. Details of our evaluation process and its limitations are provided in Tab A.

2. Our evaluation confirmed that we remain unable to adequately achieve the FMFIA objective of reliable financial reporting. Tab B provides material weakness details. Unreliable financial reporting results from our dependence on the Department of Defense (DoD) systems with systemic weaknesses, and from our inability to fully support the data underlying our inputs to these systems. Dependence on unreliable DoD financial reporting systems, first reported in FY 2003, continues to be a material weakness. Unreliable financial reporting also results from our inadequately supported and reconciled financial data. We have decided to include these in FY 2004 as management control weaknesses and added a supplemental at Tab C. Management control weaknesses differ from material weaknesses because they are within our ability to correct, are fully planned for correction, are scheduled and are in the process of being corrected.

3. I believe DIA personnel are fully committed to using strong management controls to achieve the mission entrusted to us and to protect our personnel and our homeland. Tab B contains a summary of the many significant actions and accomplishments taken to improve DIA's management controls during the past year. Management controls are accepted as an integral part of efficiently and effectively achieving our objectives and of discouraging fraud, waste, abuse and mismanagement.

enclosures a/s

L. E. Jacoby
Vice Admiral, U.S. Navy
Director

TAB A
THE EVALUATION PROCESS

Evaluation Criteria. The Defense Intelligence Agency's (DIA) senior management evaluated the system of management controls in effect during the fiscal year (FY) ending 30 September 2004. The evaluation was done in accordance with the Federal Managers' Financial Integrity Act (FMFIA) of 1982. The FMFIA directs Office of Management and Budget (OMB) to provide guidance, which it did in OMB Circular No. A-123, "Management Accountability and Control," 21 June 1995. The FMFIA further requires that OMB guidance conform to Government Accountability Office (GAO) standards. GAO provided standards in "Standards for Internal Control in the Federal Government," and "Internal Control Management and Evaluation Tool." The Department of Defense (DoD) provided its implementing guidance in DoD Directive 5010.38, "Management Control Program," 26 August 1996, and DoD Instruction 5010.40, "Management Control Program Procedures," 28 August 1996. This evaluation was part of DIA's complete revision of the entire management control process during FY 2004.

Evaluation Objectives. The objectives of DIA's evaluation were to determine whether management controls were in place and working to provide reasonable assurance that:

- Programs achieved their intended results
- Resources were used consistent with agency mission
- Programs and resources were protected from waste, fraud, and mismanagement
- Laws and regulations were followed
- Reliable and timely information was obtained, maintained, reported and used for decision making

Evaluation Limitations. This entire evaluation process is limited, and this limitation is acknowledged in the term "reasonable assurance." Assurance may be either absolute or reasonable. With absolute assurance, the result is guaranteed under all circumstances. With reasonable assurance, the result is an opinion of a likely outcome. The opinion on which the reasonable assurance is made must include consideration of the evaluator and the testing, the characteristics of fraud and the cost of controls.

The evaluator must be qualified to judge the results of the evaluation and exercise professional care in performing the evaluation. The evaluator must obtain sufficient, competent evidence to provide a reasonable basis for forming an opinion. Evidence comes from testing a sample. Testing involves judgment regarding the areas to be tested; the nature, timing, and extent of the tests to be performed; interpreting the results of the tests; and predicting the outcome of future events (results of taking differing courses of action). Predicting future events is complicated by

the risk that procedures become inadequate or compliance deteriorates. Further, errors or irregularities go undetected because of inherent limitations in management controls, resource constraints or congressional restrictions. As a result of so many instances where judgment is required and circumstances are beyond control, the evaluator relies on evidence that is persuasive rather than convincing.

Further, the characteristics of fraud, particularly those involving concealment and falsified documentation, may prevent a properly planned and performed evaluation from accurately reporting the true state of events and detecting a material misstatement.

The concept of reasonable assurance also implicitly recognizes that the cost of management controls should not exceed expected benefits. Therefore, statements of reasonable assurance are limited statements, the evaluator is not an insurer and the evaluation is a reasonable opinion and not an absolute guarantee.

Evaluation Methodology. The 2004 evaluation was supported by an entirely new management control (MC) organization and a new MC process. The organization is described in Tab B, "MCP and Related Accomplishments." The new process included assigning new responsibilities throughout the organization and having each DIA major organization produce an organizational statement of assurance (SOA). Each organization appointed and had trained an organizational Management Control Program (MCP) coordinator. Each of these coordinators used an IBM-developed MCP Self-Assessment Survey Tool to self-assess their organization. The survey tool was designed to provide an objective "current state" measurement of the organization's MCP. The survey tool's objective was to help managers evaluate their program and answer internal control questions about whether: (1) internal controls were designed well, (2) internal controls were functioning as designed and (3) further improvements were needed to internal controls. The survey tool was based on GAO's "Standards for Internal Control in the Federal Government," and "Internal Control Management and Evaluation Tool." The survey comprised three areas: (1) progressive environment, (2) business risk environment and (3) management control environment. The progressive environment assessed whether management had established a positive and supportive environment toward internal control and conscientious management. The business risk environment assessed identification, analysis, ranking and mitigation of risks. The management control environment assessed whether controls are carried out. A performance score was provided for each section. Scores ranged from a Level 0 (new or poor understanding of requirements) to Level 3 (advanced organization).

The 2004 evaluation also included several contributing considerations. Every major organization participated in providing an organizational SOA certified by the organizational head. The entire agency was inundated in multiple media with information about the MCP. Current employees were reached with our organizational publication, the *Communique* (July), which included an understandable two-page article explaining the MCP. New employees will be reached because that two-page article is now included in the training manual that all employees receive in their DIA 101 orientation training. Further, the results of internal and external reviews were included and are discussed in CORROBORATING INDICATORS, and various organizations have undertaken multiple significant improvements to the program, which are detailed in Tab B, "MCP and Related Accomplishments."

Evaluation Conclusion. This evaluation, performed within described limitations, resulted in a limited SOA. The results indicate that DIA's system of management controls in effect during the fiscal year that ended 30 September 2004, taken as a whole, provided reasonable assurance that DIA achieved four of the objectives of the FMFIA by ensuring obligations and costs complied with law, assets were safeguarded, programs achieved their intended results and resources were protected from fraud, waste, and mismanagement.

DIA was unable to adequately achieve the FMFIA objective of reliable financial reporting. Unreliable financial reporting results from our dependence on DoD systems with systemic weaknesses and from some inadequately supported data underlying our input to the systems. Dependence on unreliable DoD financial reporting systems is beyond our ability to correct and continues to be reported as a material weakness. This DIA material weakness is also reported by DoD as a systemic material weakness that applies across the department. Weakness details are provided in Tab B. The unreliable financial reporting resulting from some inadequately supported and reconciled financial data is locally reported as a management control weakness. Management control weaknesses are those that do not require reporting and assistance from outside of DIA. Management control weaknesses are within our ability to correct and are fully planned for, scheduled and in the process of being corrected. Tab C provides details of our management control weaknesses.

The self-assessment tool scoring indicated an overall 9 percent increase over 2003 in the level of DIA's performance. The progressive environment and controls assessment each improved over 2003 and remained at the intermediate (moderate) level. Risk assessment improved significantly over 2003 but still remains at the low (basic) level and is specifically targeted in 2005 for correctives.

CORROBORATING INDICATORS

Internal Reviews

Office of the Inspector General, Audits. During FY 2004, the Office of the Inspector General (OIG), Audits Unit, published 11 audit, evaluation and review reports. Under GAO and DoD IG audit procedures, OIG audits address management controls as part of their assessments. None of the 11 reports identified a material weakness in DIA's policies, procedures or practices. However, their "DIA OIG Response to Federal Information Security Management Act" report (Project Number 04-2320-OA-006) identified weaknesses that the Chief Information Assurance Officer (CIAO) addressed as "management control weaknesses." This was included as a management control weakness in Tab C. There was no other separate OIG input that would require a further limitation on the Director's SOA.

OIG, Inspections, Intelligence Oversight and Investigations. The OIG, Inspections, Intelligence Oversight and Investigations Unit, published 23 inspections, assessments and investigations. OIG investigates specific allegations of wrongdoing rather than

evaluating entire programs or processes. Therefore, their investigations may not address the adequacy of internal controls. Property management at the U.S. defense attaché offices was a recurring issue that is included in the "Reliability of Financial Information (Property, Plant and Equipment)" management control weakness in Tab C. There was no other separate OIG input that would require a further limitation on the Director's SOA.

External Reviews

DoD IG. DoD IG issued one audit and one evaluation report to DIA during FY 2004. The audit report identified material management control weaknesses in DIA.

"Reliability of the Defense Intelligence Agency FY 2003 Financial Statements" (D-2004-079, 29 April 2004). The report stated, "Although DIA made improvements in the presentation of its FY 2003 financial statements, the reliability and accuracy of information used to prepare and report annual financial statements continued to be questionable. DIA management has recognized the importance of the accuracy and reliability of its financial information and began to take actions during FY 2003 to enhance the reliability of its financial statements. Despite significant challenges, we believe that DIA is making progress in improving its financial reporting, and in moving toward the goal of producing auditable financial statements."

"Most of the deficiencies relating to property, plant, and equipment identified in the prior Inspector General of the Department of Defense audit reports have not been corrected. Also, during FY 2003, we identified additional deficiencies related to accounting for and reporting of property, plant, and equipment. Specifically, DoD did not complete an inventory of all property, plant, and equipment; maintain proper support on acquisitions and record the acquisition cost correctly; complete investigations of lost property; report all capital property; and record depreciation correctly. Until improvements in internal control over accounting for and reporting of capitalized property are made and fully implemented, the amount reported for property, plant, and equipment on the balance sheet will not be complete and verifiable."

"To improve the reliability of the DIA financial statements, DIA needs to implement recommendations from prior Inspector General of the Department of Defense audits and fully comply with the Office of Management and Budget and DoD guidance when preparing the annual financial statements. DIA should establish controls to ensure that deficiencies relating to accounting for and reporting of capital assets are corrected. In addition, DIA should train property personnel responsible for accounting for and reporting of capital assets."

"We identified material management control weaknesses as defined by DoD Instruction 5010.40, "Management Controls Program Procedures." Management controls at DIA were not adequate to ensure that the financial statements were an accurate and reliable representation of the financial operations at DIA. Specifically, DIA lacked adequate management controls related to the reconciliation of Fund Valance with Treasury, Obligations, Accounts Payable, and PP&E."

"DIA did address the material weaknesses related to the financial system in its FY 2003 Annual Statement of Assurance. However, DIA did not address the material control weaknesses related to the financial statement preparation process, the reconciliations, and the review of unliquidated obligations. Also, DIA did not acknowledge material control weaknesses with PP&E in the FY 2003 Annual Statement of Assurance."

"Effectiveness of the Joint Reserve Intelligence Centers' Support to the Warfighter" (04-INTEL-13, 30 June 2004). This report was an evaluation report and did not contain any comments on management controls or material weaknesses.

DoD SYSTEMIC WEAKNESSES

Reporting Requirement. DoD Directive 5010.38 requires that the Office of the Secretary of Defense (OSD) principal staff help identify and/or report the status of "systemic weaknesses" that fall within their area of functional responsibility. Systemic weaknesses occur from two sources. First, systemic weaknesses result when management control problems are reported to the Secretary of Defense (SECDEF) by more than one DoD component and the weakness is determined by SECDEF or his deputy to potentially jeopardize the department's operations, which can result in significant instances of fraud, waste, abuse or other violations of the public trust. Second, the OSD principal staff can identify new systemic management control weaknesses for inclusion in the DoD annual SOA, either because the weakness in management controls cuts across areas of functional responsibility or is occurring in more than one DoD component. All DoD components are required to list each OSD systemic weakness reported in the FY 2003 DoD SOA and list any of the components' weaknesses that are related to the systemic weaknesses.

DoD Financial Management Systems and Processes. "DoD financial and business management systems and processes are not fully integrated and do not provide information that is reliable, timely and accurate. The estimated correction date is 4th Qtr FY 2006."

DIA has identified the absence of an overarching approach to financial management as a material weakness preventing DIA from passing financial audits and obtaining a "clean" audit opinion. This reporting is done in Tab B. Related financial management systems and processes management control weaknesses are listed in Tab C.

Management of Information Technology and Assurance. "DoD needs to better manage information technology and needs assurance that information technology is adequately protected. The estimated correction date is 3rd Qtr FY 2007."

The DIA CIAO has not declared this to be a DIA material weakness. This decision was based on some of the many improvement initiatives that are detailed in Tab B, "MCP and Related Accomplishments." The July 2004, DIA OIG Federal Information Security Management Act independent evaluation (Project 04-2320-OA-006) did identify two weaknesses but did not categorize them as material weaknesses. The CIAO identified these same weaknesses as management control weaknesses and these are included in Tab C.

Environmental Liabilities. "The DoD has not developed the policies, procedures and methodologies needed to ensure that cleanup costs for all of its ongoing and inactive or closed operations are identified, consistently estimated and appropriately reported. Site inventories and cost methodologies to identify budget requirements and financial liabilities continue to need improvement. The estimated correction date is 1st Qtr FY 2004."

This issue does not apply to DIA. At the single location that could have a potential liability, there is an interservice support agreement that transfers responsibility for environmental issues to the host installation.

Personnel Security Investigations Program. "DoD hiring is adversely affected because personnel security investigations are backlogged. The estimated correction date is 4th Qtr FY 2004."

This issue does impact DIA, but management did not declare this as a material weakness. This decision was based on some of the many improvement initiatives undertaken to help offset the clearance delays, which are detailed in Tab B, "MCP and Related Accomplishments."

Real Property Infrastructure. "The department has not adequately managed the real property infrastructure to halt the deterioration or obsolescence of facilities on military installations. The estimated correction date is 1st Qtr FY 2006."

This weakness does not apply to DIA. Over the last year, the agency invested millions of dollars in recapitalizing the support infrastructure and renovating portions of the DIA headquarters facility and surrounding structures throughout the DIA campus on Bolling Air Force Base. In April 2004, DIA replaced the previous maintenance force with a contracted maintenance force under the Regional Base Operations Services and Support (RBOSS) contract. Since April, DIA has developed an extensive preventive maintenance and recapitalization program under the RBOSS contract.

Contracting for Services. "Acquisition oversight is not always adequate when contracting for DoD services and can result in failure to obtain the best value on individual procurements. The estimated completion date is 2nd Qtr FY 2005."

This weakness does not apply to DIA. The Chief for Procurement retained a private company to perform a Quick-Look "AS IS" assessment of DIA's acquisition system, including adherence to federal acquisition regulations and external regulations and policies. The DoD-wide systemic weakness was not specifically noted as one of the 20 weaknesses identified in the final report.

Government Card Program Management. "Instances of misuse, abuse, and fraud in respect to purchase and travel card use have been attributed to inadequate DoD emphasis on proper use of the cards, poorly enforced controls, and lax oversight."