



DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-

1 October 2003



U-2531/FE-2B

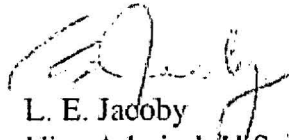
MEMORANDUM FOR THE SECRETARY OF DEFENSE

SUBJECT: Annual Statement Required Under the Federal Managers' Financial Integrity Act (FMFIA) of 1982

As Director of the Defense Intelligence Agency (DIA), I recognize the importance of management controls. I have taken the necessary steps to ensure a conscientious and thorough evaluation of management controls for DIA. The results indicate that the DIA system of internal accounting and administrative control, in effect during the fiscal year ending September 30, 2003, provides reasonable assurance, with the exception of the material weakness noted, that management controls are in place, being used, and operating effectively. Furthermore, DIA achieved the FMFIA objectives within the limits described in Tab A, which also provides information on how DIA conducted the evaluation and cites any deficiencies found in the process.

The evaluation did identify a material weakness that still requires corrective action (Tab B-1). Tab B-2 is an individual narrative on this weakness. Tab B-3 shows no material weaknesses were identified as corrected. At Tab B-4 is a summary of the significant accomplishments and actions taken to improve Component management controls during the past year.

Attachments:  
As stated

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

## **The Concept of Reasonable Assurance And How the Evaluation Was Conducted**

1. The system of internal accounting and administrative control of the Defense Intelligence Agency (DIA) in effect during the fiscal year ending 30 September 2003, was evaluated in accordance with the guidance provided by Office of Management and Budget Circular (OMB) A-123 (Revised), Management Accountability and Control, 21 June 1995, as implemented by DoD Directive 5010.38, Management Control Program, 26 August 1996 and DoD Instruction 5010.40, Management Control Program Procedures, 28 August 1996. The OMB guidelines were issued by the Director of the Office of Management and Budget, in consultation with the Comptroller General, as required by the Federal Managers' Financial Integrity Act of 1982. Included is an evaluation of whether the system of internal accounting and administrative control of the DIA is in compliance with standards prescribed by the Comptroller General.

2. The objectives of the system of internal accounting and administrative control of the DIA are to provide reasonable assurance that:

- a. Obligations and costs are in compliance with applicable law.
- b. Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation.
- c. Revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

3. The evaluation of management controls extends to every responsibility and activity undertaken by DIA and is applicable to financial, administrative, and operational controls. Furthermore, the concept of reasonable assurance recognizes that (1) the cost of management control should not exceed the benefits expected to be derived and (2) the benefits consist of reductions in the risks of failing to achieve the stated objectives. The expected benefits and related costs of control procedures should be addressed using estimates and managerial judgment. Moreover, errors or irregularities may occur and not be detected because of inherent limitations in any system of internal accounting and administrative control, including those limitations resulting from resource constraints, Congressional restrictions, and other factors. Finally, projection of any evaluation of the system to future periods is subject to risk that procedures may be inadequate because of changes in conditions, or that the degree of compliance with procedures may deteriorate. Therefore, statements of reasonable assurance are provided within the limits of the preceding paragraph.

4. The evaluation was performed in accordance with the guidelines identified above. The results indicate that the system of internal accounting and administrative control of the DIA in effect during the fiscal year that ended 30 September 2003, taken as a whole, complies with the requirement to provide reasonable assurance that the above mentioned objectives were achieved with the exception of financial management systems and processes. This position on reasonable assurance is within the limits described in the preceding paragraph.

5. DIA is divided into assessable units along organizational lines reflecting the major components of the Agency. This assessable unit structure is reflected in the DIA annual Management Control Plan. DIA will evaluate the assessable unit structure along functional lines in FY04.

6. In addition, the General Account Office (GAO) has issued its "Standards for Internal Control in the Federal Government" (GAO/AIMD-00-21.3.1, November 1999). Those standards identify the overall framework for establishing and maintaining internal control and for identifying and addressing major performance challenges and areas of greatest risk for fraud, waste, abuse and mismanagement. The GAO also has issued an "Internal Control Management Evaluation Tool" (GAO-01-1008G, August 2001) to assist agencies in maintaining or implementing effective internal control. DIA used this tool in performing our self-assessment.

**Office of the Secretary of Defense (OSD) Systemic Weakness Disclosure:**

DoD Directive 5010.38 requires that OSD Principal Staff Assistants (PSAs) identify and report "systemic weaknesses" that fall within their area of functional responsibility. Systemic weaknesses are management control problems identified by more than one DoD Component that are judged to be of such consequence as to potentially jeopardize the Department's operations or result in significant incidences of fraud, waste, abuse or other violations of the public trust. OSD Principal Staff Assistants (PSAs) forwarded narratives identifying OSD systemic weaknesses. Those systemic weaknesses applicable to DIA are addressed below.

## Defense Intelligence Agency Financial Management Systems and Processes

Like the Department of Defense, the Defense Intelligence Agency (DIA) financial management systems and business processes do not provide accurate, reliable and timely information, thus hindering effective management decision-making. The current financial environment is comprised of many discrete systems characterized by poor integration and minimal data standardization. This absence of an overarching approach to financial management is a major obstacle preventing DIA from passing financial audits and makes this a material weakness.

### Impact:

DoD continued, an inferior financial management information infrastructure hinders the efficiency and effectiveness of DIA's operations and prevents managers from making more timely and cost-effective decisions. The substandard financial management processes and information infrastructure, and the previous absence of an agency-wide, integrated approach to financial management, also contributed to the following difficulties:

- Overly complex data requirements that are driven by appropriation funding rules, elaborate policies and procedures, and outdated guidelines for excessively detailed tracking of expenditures.
- Convoluted business processes that fail to streamline excessive process steps that are further complicated by aged and disparate systems (accounting, financial and nonfinancial ("feeder")).
- Inability to meet evolving federal financial management standards.
- Difficulty in obtaining financially based, outcome-oriented, metrics for
- Decision makers. Many of the metrics currently in use reflect weak links between annual performance goals and outputs.
- Inability to produce annual financial statements that result in an unqualified audit opinion.
- Personnel who lack the technical skills necessary to support and maintain integrated financial management systems and operations.

### Management Response:

DIA is improving its financial management processes, systems, and information by engaging in a number of wide-ranging initiatives:

DIA developed and briefed to OMB a plan to improve our financial management systems, information. This plan is to help implement the President's Management Agenda goals of Improved Financial Performance and Budget and Performance Integration. At the end of the fourth quarter in 2003, DIA has accomplished more than planned.

DIA is participating in the SecDef's recently established Financial Management Modernization Program to direct and oversee financial management reform within the Department. DIA has representatives in the Accounting and Strategic Planning and Budgeting Domains. DIA hosted the DoD members of the Intelligence Community in a Classified Line of Accounting meeting, as part of this initiative. DIA continues supporting this DoD-wide management approach to improving business processes and implementing integrated financial management systems.

- DIA is also participating in National Security Agency (NSA) Working Groups, as part of NSA's efforts to develop the Intelligence Financial Management Enterprise System Pilot

for DoD. DIA is improving its own processes and legacy systems to improve the timeliness, accuracy, and relevancy of its financial management information and to aid in transitioning to the NSA and/or DoD enterprise architecture. Significant accomplishments within the last 30 days include standardization and future availability of integrated programming, budgeting and execution data. DIA is dependent on NSA's successful implementation of a new accounting system.

- DIA recently began obtaining outside advice from other federal agencies and professional audit firms to determine the necessary action to receive a "clean" opinion on audited financial statements.
- DIA is obtaining the consulting services of a professional audit firm to help develop a road map to implement all standards required for a "clean" financial opinion at the earliest opportunity.
- DIA is firmly committed to resolving auditor-identified and Federal Managers Financial Integrity Act of 1982 material weaknesses in internal controls.
- DIA has already implemented internal control recommendations contained in a June 2003 DIA Inspector General (IG) report on the Internal Control Management Program.
- DIA has already begun implementing the internal controls for improving fund distribution and reducing potential erroneous payments contained in the April 2003 Department of Defense (DoD) Inspector General (IG) Report.
- DIA established a new division (FE-4) to develop, track, and report monthly financial and performance information for routine use during operational evaluation and decision-making.
- DIA has developed financial performance metrics and General Defense Intelligence Program (GDIP) performance metrics and plan to make them available on line for the DIA Director, Chief Financial Executive (CFE), senior managers, and program and budget analysts. Included in this effort is contractor support to automate the collection of daily financial performance metrics and make it available on line.

Planned Actions:

- Complete a DIA Chief Financial Officers Strategic Plan to develop and begin implementing a complete road map for DIA enterprise architecture with integrated systems, improved processes, and standardized data, in order to obtain accurate, reliable and timely information supporting effective management decision-making and passing financial audits.
- Continue participating at Planning and Budgeting Domain Working Groups as part of the Office of the Secretary of Defense, Comptroller's Financial Management Enterprise Architecture.
- Continue participating at NSA workshops for developing a replacement of existing budget and accounting systems and an enterprise architecture.
- Continue developing an interface between NSA's financial system and DIA's

programming and budgeting systems.

- Conduct second quarterly in-process-review (IPR) of DIA financial system enhancements. Include a review of the contractor's financial statement road map.
- Review implementation of interface for two of DIA's manpower systems. Begin developing an interface for the third manpower system.
- Begin Phase 1 of a three phased implementation of the interface for DIA's financial systems.
- Begin implementing the independent audit contractor report containing a detailed and comprehensive road map of the work required to obtain a "clean" opinion on DIA's financial statements.
- Review standardized DIA line of accounting and begin development of an interface to eliminate double data entries.
- Continued bi-weekly meetings with DIA managers to implement an integrated DIA financial statement enterprise architecture.
- Continue to reengineer DIA's financially related business processes to ensure routine availability of reliable, accurate and timely financial management information.
- Begin using automated financial performance metrics and make available on line at DIA for Director to CFE to senior managers to budget analysts.
- Begin automating financial *and non-financial* performance metrics and plan to make available on line at DIA for Director to CFE to senior managers to budget analysts for monthly reporting.
- Develop a capital investment strategy and investment plan that includes costs, people, policies, processes and systems for the Department's transition to a fully integrated financial management system that is compliant with applicable federal and DoD standards.

## **Defense Intelligence Agency Information Assurance (IA)**

Defending our information systems and ensuring their integrity is an ongoing effort that is crucial to the success of our missions and the security of our Nation. This effort faces intensified challenges as a result of the changing environment in which we work. Our government has minimized the ownership of its information infrastructure and expanded its reliance on a commercially based information environment. These actions, in conjunction with the increasing sophistication and availability of technologies that can be accessed and used against us by potential adversaries, have heightened our information networks' vulnerability to hostile actions by external and internal parties. In order to address these issues, as well as any other real and perceived threats to achieving and maintaining our information superiority over current and future enemies, we must develop, institute, and aggressively enforce information assurance programs.

### Impact:

A successful attack on Joint Worldwide Intelligence Communication Systems (JWICS) would have a serious and immediate impact on the ability of Department of Defense Intelligence Information Systems (DoDIIS) to carry out its mission.

### Management Response:

In order to implement a well-designed, enterprise-wide IA program which ensures that proper security controls are consistently applied across the community, DIA will:

- Implement an enterprise-wide vulnerability assessment and risk analysis to determine Community strengths and weaknesses
- Institutionalize metrics and measurement process to continue determining effectiveness of the Program
- Create a program to assess compliance, overall effectiveness, and evaluate future IA initiatives
- Begin assessing an insider threat profile to give DIA a proactive capability
- Provide security engineering professionals to design and incorporate security as part of life cycle management
- Establish a Community outreach program for knowledge sharing, incident coordination, reporting, and situational awareness
- Provide training requirements for IA practitioners, systems administrators, operators and users

### Planned Actions:

The DIA will:

- Update DIA IA Policy document, DIAM 50-4 by FY04
- Create a repeatable set of Certification & Accreditation (C&A) business processes with IA vulnerability tools supporting centralized management and decentralized IA execution for the by FY04
- Deploy vulnerability assessment and risk analysis technologies to DoDIIS sites by end of FY04
- Identify and correct SANS/FBI (Sys Admin, Audit, Network, Security) top twenty (20) vulnerabilities on the DoDIIS SCI network by end of FY04
- Increase the number of trained personnel for IA by 40% by end of FY04
- Provide means for DIA NIPRNet account holders to get class 3 PKI software certificates by FY04
- DIA will continue to publish an IA Annual Report

## Defense Intelligence Agency Environmental Liability

The Defense Intelligence Agency (DIA), Missile and Space Intelligence Center (MSIC) obtains munitions samples as part of its Foreign Materiel Exploitation (FME) program. Storage of these munitions items is in accordance with DoD guidelines and in conjunction with U.S. Army facilities available at Redstone Arsenal, Huntsville, Alabama. Many of the munitions obtained under the MSIC FME program could contain hazardous chemicals (i.e., rocket fuels) and explosives (e.g., warheads, squibs, etc.) as well as hazardous materials (e.g., radiological devices) which require proper handling, storage and disposal in accordance with DoD and Army regulations.

### Impact:

Recent munitions acquisitions obtained from Iraq, along with other munitions obtained as part of the ongoing DIA FME program, require proper preparation before exploitation of the weapon systems capabilities. To date, MSIC has met all the environmental requirements set forth by the DoD, U.S. Army and Redstone Arsenal. Certain environmental liabilities remain with munitions that were obtained rapidly from the short Iraq war.

### Management:

Management actions to date include:

- MSIC has inventoried all FME equipment which may pose an environmental liability. This is particularly so with the large volume of equipment recently obtained from Iraq.
- MSIC has developed plans for properly disposing of all FME equipment (and/or components) which may pose an environmental liability.

### Planned Action:

DIA planned actions include:

- MSIC will continue to inventory any newly acquired Iraqi equipment and other FME acquisitions.
- MSIC will develop plans, as needed, for properly disposing of any hazardous items in Iraqi equipment and other FME systems which may pose an environmental liability.
- In accordance with newly established DoD policies, MSIC will estimate the costs for disposing (and/or rendering environmentally safe) the newly Iraqi equipment and other FME systems.
- MSIC will continue to work with U.S. Army Redstone Arsenal personnel to ensure compliance with all environmental liabilities guidelines.

**Defense Intelligence Agency  
Management of Munitions and Explosives**

1. Not Applicable. DIA is fully cognizant of range management issues involving munitions and we conduct our operations on the Army's ranges to facilitate range compliance with their munitions management responsibilities.

**Defense Intelligence Agency  
Personnel Security Investigations (PSI) Program**

DoD continues to struggle to achieve an efficient and effective personnel security investigations program. In pursuit of this goal, the department is transforming the process via the transfer of the security background investigation mission to OPM, effective 01 October 2003.

Impact:

DIA and its Defense component customers will continue to suffer from extended PSI completion rates during the divestiture process. As an example, the OPM completion rate for "guaranteed" 75 day cases is currently running at 248 days.

Management Response:

Counterintelligence and Security Activity (DAC) has undertaken several initiatives to help offset the clearance delays caused by cited circumstances:

- In June 2003, DAC received OSD approval to expand the use of its contract Background Investigations Provider (BIP) through FY 04. The DIA BIP provides expeditious security investigation completion rates of 30-40 days for DIA applicant cases. Expansion of this authority will permit DAC to effectively support the current and anticipated applicant surge demands.
- DAC has also extended the use of the BIP services to cover, on a shared contract basis, a Defense component requirement for expeditious completion times.
- DAC has recently acquired several contractor assets to increase the responsiveness of its case management and control process. The accession of contractor personnel permits permanent central clearance staff to concentrate on direct adjudication support and clearance issuance.
- More frequent use is being made by DAC of its Accelerated Clearance Eligibility (ACE) procedure whereby expeditious National Agency Checks are conducted and access eligibility granted while the BIP is conducting the fast-track background investigation.

Planned Actions:

DAC continues to explore new, improved methods to streamline clearance demands from unanticipated surges such as staffing of the Iraqi Survey Group. In FY 04, additional contractor personnel will be added to the central clearance office to handle administrative portions of the clearance process. Discussions are also underway with one customer defense component that seeks to fund a contractor billet to administer the DAC workload pertaining to that customer agency. Separately, two customer defense components have indicated interest in utilizing the services of DAC's BIP to conduct, on a shared contract basis, background investigations on limited numbers of high priority cases in those agencies. DAC is also adding a contractor to facilitate a review of the cradle to grave business process review of the Personnel Security Investigations Program.

## Defense Intelligence Agency Real Property (Facilities) Infrastructure

The Defense Intelligence Agency (DIA) recognizes the importance of maintaining its infrastructure to support the mission, health and safety of personnel and recapitalization of assets. Currently, the agency has an aggressive preventive maintenance program that provides routine inspections, repairs and replacement of worn operational components and architectural features.

### Impact:

Failure to adopt and incorporate an active facility maintenance program could result in unreliable infrastructure that would adversely affect the mission and personnel effectiveness:

### Management Response:

"Over the last year the agency made a significant investment to enhance facility maintenance and support capital improvement projects. In addition, DIA completed an extensive recapitalization initiative that assessed the condition of all facility and support components. Each component was given a facility condition index and cataloged into a data model to provide budget forecasts and assist in scheduling the preventive maintenance and replacement of facility support assets before components reach their designed life span.

In FY04, the agency plans to continue investments to further recapitalize its infrastructure."

### Planned Actions:

DIA continues to enhance its facility maintenance and management operations. Currently, the agency has several on-going projects that are designed to optimize the efficiency of facility maintenance and facility operations.

- Adopt the Regional Base Operating Support (RBOS) contract for facility operations and maintenance in April 2004. RBOS will improve operational support and preventive maintenance at the DIA headquarters facility on BAFB.
- Incorporate results from an on-going Comprehensive Facility Maintenance Program (CFMP). The CFMP is designed to review and compare existing facility maintenance procedures and processes with industry standards and provide recommendations to enhance overall facility maintenance and operations.
- Complete procurement of the web-based software that will provide real-time data on facility conditions.
- Manage several scheduled capital improvement projects such as replacing escalators, UPS system, Power Distribution Units, upgrading lighting and HVAC in the Cafeteria.

**Defense Intelligence Agency  
Contracting for Services**

Impact:

An assessment of DIA's Acquisition System was completed in 2003. The assessment evaluated agency organization, policies, processes, training, tools and references that support the acquisition of supplies and services in light of best practices. Twenty recommendations and a plan of action and milestones provided a roadmap for improvement of systemic weaknesses. One recommendation that the agency implemented to improve the contracting of services is the establishment of a Component Acquisition Executive (CAE) who reports to the Deputy Director and the subsequent realignment of the Contracting Office to the Command Element reporting directly to the (CAE). Establishment of a single point of leadership is a clear signal of DIA's commitment to a strategic approach to the acquisition of services and the required enforcement of acquisition laws, policies and procedures.

Management Response:

To improve its intelligence support, add alternatives to deploying the right skill mix and capability to operational requirements, and correct systemic contracting weaknesses, DIA requested, and expect to receive next fiscal year, statutory authority to enter into personal services contracts. DIA would use the authority sparingly and only when the agency must carry out work for a temporary period which cannot be delayed because of a critical need; and the need cannot be met with current employees or through the direct appointment of temporary employees within the time available, and the duration of time, help is needed. For example, the authority would be useful in support of the hunt for WMD in Iraq and similar operations in support of the Global War on Terrorism.

Planned Action:

Recent procurement legislation increased the single use limit of the Government Purchase Card from \$2,500 to \$15,000 in time of contingency and up to \$250,000 in overseas contingency contracting situations. This limit increase has multiplied the utility of the purchase card for DIA and commercial sources. In fact, a DIA lesson learned from Operation Iraqi Freedom, is that the Purchase Card was not only an invaluable tool to expedite contracting support in theatre, but also the preferred method of contracting by local sources there. DIA's approach to managing the Purchase Card program includes vesting accountability for the Purchase Card authority with the Head of the Contracting Activity and assigning Purchase Card Program Management to a designated program manager in the DIA Office for Logistics that is a separate office from the Contracting Activity. This management control system, along with vigorous financial management oversight by DIA's Accounting Division, provides a very robust check-and-balance system to facilitate acquisition planning, streamline the accounting processes, and prevent potential abuse of the purchase card.

## Defense Intelligence Agency Government Card Program Management

### Travel Charge Cards

The areas of concern with the DoD Individually Billed Accounts (IBA) travel charge card program are misuse and late payment or non-payment by military members and civilian personnel of travel charge card debt owed to the vendor bank. DIA's performance has been progressively improving. As of August 2003, past due accounts which are 60 or more days overdue represent 1.2% of open agency accounts (adjusted for accounts in mission critical status). Also, inappropriate use of the travel charge card has been documented. Travel charge cards are to be used only for expenses incurred in connection with official government travel.

#### Impact:

Delinquency and misuse can impact an individual's creditworthiness and trustfulness, which are major components when reviewing suitability for TS/SCI-level security clearances.

#### Management Response:

FE-3 is working aggressively to monitor all agency accounts to ensure that they are used appropriately and balances due are paid in a timely manner. As part of our program, we have:

- Established points of contact in each key component (KC) to keep open lines of communication between financial management personnel and staffers in the directorates. This ensures that problems are identified and corrected quickly.
- Prepared, analyzed and distributed the monthly delinquency report to each KC with employees who have past due accounts. Requested follow-up from each KC to explain the reason for the delinquency and steps taken to correct the problem.
- Performed data mining activities via software scans to look for suspicious activity. Sends information to IG, DAC, KC and supervisor of employee for follow-up. Disciplinary actions are taken, including removal for offenders.

#### Planned Actions:

FE-3 will continue to monitor cardholder accounts for any improper usage and continue to work delinquency lists to keep to a minimum past due accounts, while providing timely customer service to help cardholders with problems. We are researching the possibility of turning day-to-day charge card program operations over to a contractor. This will allow FE-3 personnel to do more extensive data mining and other account maintenance projects, as well as participate more fully at DoD/DFAS level in the process.

### IMPAC Program

The Defense Intelligence Agency continues to improve the management and control of the International Merchants Purchase Authorization Card (IMPAC) program while expanding its use. During the past year, the program management has been increased through the introduction of an assistant program manager, and an internal review inspector. The Agency has made available this past year the use of a web enabled purchase register to track funds allocations and expenditures by the IMPAC cardholders and approving officials. Use of the automated purchase

register will be made mandatory for the next fiscal year, permitting data mining and additional programmatic oversight previously unavailable to the program manager.

Impact:

The Defense Intelligence Agency has placed significant emphasis on the management and controls over the IMPAC program. Annually the Inspector General focuses an audit on the IMPAC program. Recent audit reports have predominantly only noted minor problems. While the potential for the abuse exists within the program, the DIA checks and balances make it more difficult for the government to experience a significant loss without being discovered. Significant emphasis is placed on training both cardholders and billing officials on their duties, responsibilities and financial liability. DoD audits have indicated *Failure of management controls also undermines the ability of the Government to seek adjustments for billing errors or fraudulent purchases that were not made by the cardholder. In addition, the failure of management controls could result in the government not obtaining the best possible price.*

Management Response:

As the Agency pursues a constant improvement process with the IMPAC program, it has recognized additional controls are required to ensure all billed purchases are true and accurate. To date the effort has been to ensure adequate training and oversight is provided to both the cardholder and the billing official. Future plans include an automated reconciliation performed by downloading the bank statement and comparing the billed amount to the amount recorded for the purchase in the automated purchase register. This same solution will be used to improve the processing time required to submit for payment the IMPAC bill. Improved bill processing will enable the maximization of rebates for prompt payment. Additional training on proper use and controls for the IMPAC card program are planned for the next FY, including refresher training, and training on ensuring the government is receiving the best possible price for the goods and services received through the IMPAC program. The Agency Program Management staff has been increased by two key positions, providing additional guidance and an internal inspection capability to the program. These actions will have a stabilizing effect on the program along with increasing the visibility of the oversight function.

Planned Actions:

- Make mandatory the use of the web enabled IMPAC purchase register
- Develop and implement an automated reconciliation of the bank statement billed amount to the purchase register
- Improve the payment processing through use of an automated reconciliation process.
- Enhance the refresher training and increase training on obtaining best price purchases for the government
- Conduct a review of IMPAC card use during operations in Iraq

UNCORRECTED WEAKNESSES IDENTIFIED DURING THE PERIOD

<u>TITLE</u>	<u>TARGETED CORRECTION DATE</u>	<u>Page#</u>
Financial Management Systems and Processes	4 <sup>th</sup> Quarter 2006	Tab B-2

UNCORRECTED WEAKNESSES IDENTIFIED DURING PRIOR PERIODS

NONE

CORRECTED WEAKNESSES IDENTIFIED DURING ALL PERIODS

NONE

## UNCORRECTED WEAKNESSES IDENTIFIED DURING THE PERIOD

### Financial Management Systems and Processes

*Description of the Issue:* Like the Department of Defense, the Defense Intelligence Agency (DIA) financial management systems and business processes do not provide accurate, reliable and timely information, thus hindering effective management decision-making. The current financial environment is comprised of many discrete systems characterized by poor integration and minimal data standardization. This absence of an overarching approach to financial management is a material weakness preventing DIA from passing financial audits and obtaining a "clean" audit opinion.

*Functional Category:* Comptroller/Resource Manager

*Component:* Defense Intelligence Agency

*Pace of Corrective Action:*

- *Year Identified:* 2003
- *Original Targeted Correction Date:* FY 2006
- *Targeted Correction Date in Last Report:* N/A
- *Current Target Date:* FY 2006

*Validation Indicators:* Corrective action is briefed every 2 weeks to DIA Senior Executives. Also, briefed the President's Management Agenda (PMA) Item #3 on "Improved Financial Performance" status is briefed quarterly to the President's Office of Management and Budget (OMB). DIA's Financial Statements are audited annually. In addition, ad hoc DIA management reviews and Inspector General reviews have been conducted by DIA and DoD Inspector Generals.

*Result Indicators:* DIA was recently praised during the last quarterly brief for the progress and being ahead of the initial schedule.

*Source Documents:* The following sources identified this issue:

1. The President's Management Agenda - Fiscal Year 2002 (Government-Wide Initiatives)
2. Department of Defense Performance and Accountability Report - Fiscal Year 2002 (Systemic Weaknesses)
3. Department of Defense Inspector General report on Financial Management - Reliability of the FY 2002 DIA Financial Statements and Adequacy of Related Procedures and Controls

*Progress to Date:* The DIA has taken steps to correct this material weakness. These steps include:

Accomplishments for 2003:

- Continued participation in developing new financial management system.
- Contracted CPA firm for CFO support

- Established President's Management Agenda (PMA) Audit Committee charter (Federal Financial Managers Advisory Committee)
- Reviewed and updated detailed milestones
- Established training programs
- Continued work with DOD IG on FY 03 Financial Statements
- Instituted DIA Audit Committee Charter
- Provided support to program managers for tri-annual reviews
- Worked with CPA contractor to resolve issues
- Continued participating in development of new financial management system
- Worked with CPA contractor to resolve DoD IG findings/recommendations
- Established FE-4 contractor staffing
- Implemented 2nd generation CFO Council financial performance metrics report
- Established use of financial performance information for routine use in evaluation and decision making
- Develop automated financial and performance information for:
  - Quarterly spend plan reviews
  - POM submission reviews
  - Presidential Budget Submission, Congressional Budget Justification Book, and Congressional Justification Book reviews
- Refined GDIP financial and performance info
- Automated, and made available online:
  - Financial performance metrics for reporting
  - Daily financial performance metrics
- Tracking financial and non-financial metrics and planning to make available online for monthly reporting

*Additional FY 2003 Accomplishments (Not Planned):*

- Established Financial Integration Group (FIG) to begin integration of DIA financial feeder systems
- Developing interfaces to integrate DIA financial feeder systems into official accounting system
- Began development of CFO Strategic Plan
- Conducted DIA internal control training
- Began automating best practice processes for risk assessments
- Began automating best practice processes for annual Statement of Assurance
- Established and wrote Audit Committee charter, which will be used to help resolve auditor-identified deficiencies

*Major Milestones:* The following identifies the major milestones DIA plans to complete during FY 2004:

- Complete CFO Strategic Plan
- Complete Audit of FY 2003 Financial Statements
- Complete Financial Feeder System Interfaces w/official accounting system (Phase 1)
- Resolve any Agency-identified deficiencies in the FY03 CFO process to preclude recurrence in FY04
- Continue collaborative efforts with NSA for development of new financial management system (Phase 2)
- Continue work with CPA firm to resolve issues and DOD IG identified findings and recommendations

- Complete automating best practice processes for annual Statement of Assurance and for risk assessments
- Implement tasks detailed in the comprehensive roadmap in order to obtain "clean" opinion
- Complete Phase 1 of the three phased implementation of DIA's financial systems interface
- Begin developing a business enterprise architecture to include non-financial as well as financial business information required for financial statements and other external and internal management reporting (Phase 3)
- Conduct quarterly In-Process Reviews (IPRs) of DIA financial system enhancements
- Completed Automated Internal Control Self-Assessment Survey
- Automation of Best Practice Annual Statement of Assurance
- Coordinate Internal Control efforts with DoD and across DIA
- Conduct assessments of large impact and probably risk areas
- Begin automating financial and non-financial performance metrics and make available online for monthly reporting
- Continue to improve and develop new performance metrics

**UNCORRECTED WEAKNESSES IDENTIFIED DURING PRIOR PERIODS**

NOT APPLICABLE

MATERIAL WEAKNESSES CORRECTED DURING THIS PERIOD

IDENTIFIED DURING THE PERIOD: NOT APPLICABLE

IDENTIFIED DURING PRIOR PERIODS: NOT APPLICABLE

## Management Control Program and Related Accomplishments

### Financial Management Systems and Processes

#### Description:

Like the Department of Defense, the Defense Intelligence Agency (DIA) financial management systems and business processes do not provide accurate, reliable and timely information, thus hindering effective management decision-making. The current financial environment is comprised of many discrete systems characterized by poor integration and minimal data standardization. This absence of an overarching approach to financial management is a major obstacle preventing DIA from passing financial audits and makes this a material weakness.

#### Accomplishments:

DIA is improving its financial management processes, systems, and information by engaging in a number of wide-ranging initiatives:

DIA developed and briefed to OMB a plan to improve our financial management systems, information. This plan is to help implement the President's Management Agenda goals of Improved Financial Performance and Budget and Performance Integration. At the end of the fourth quarter in 2003, DIA has accomplished more than planned.

DIA is participating in the SecDef's recently established Financial Management Modernization Program to direct and oversee financial management reform within the Department. DIA has representatives in the Accounting and Strategic Planning and Budgeting Domains. DIA hosted the DoD members of the Intelligence Community in a Classified Line of Accounting meeting, as part of this initiative. DIA continues supporting this DoD-wide management approach to improving business processes and implementing integrated financial management systems.

DIA is also participating in National Security Agency (NSA) Working Groups, as part of NSA's efforts to develop the Intelligence Financial Management Enterprise System Pilot for DoD. DIA is improving its own processes and legacy systems to improve the timeliness, accuracy, and relevancy of its financial management information and to aid in transitioning to the NSA and/or DoD enterprise architecture. Significant accomplishments within the last 30 days include standardization and future availability of integrated programming, budgeting and execution data.

DIA recently began obtaining outside advice from other federal agencies and professional audit firms to determine the necessary action to receive a "clean" opinion on audited financial statements.

## Information Assurance (IA)

### Description:

A successful attack on Joint Worldwide Intelligence Communication Systems (JWICS) would have a serious and immediate impact on the ability of Department of Defense Intelligence Information Systems (DoDIIS) to carry out its mission.

### Accomplishments:

- Implement an enterprise-wide vulnerability assessment and risk analysis to determine Community strengths and weaknesses
- Institutionalize metrics and measurement process to continue determining effectiveness of the Program
- Create a program to assess compliance, overall effectiveness, and evaluate future IA initiatives
- Begin assessing an insider threat profile to give DIA a proactive capability.
- Provide security engineering professionals to design and incorporate security as part of life cycle management
- Establish a Community outreach program for knowledge sharing, incident coordination, reporting, and situational awareness
- Provide training requirements for IA practitioners, systems administrators, operators and users

## Environmental Liability

### Description:

Recent munitions acquisitions obtained from Iraq, along with other munitions obtained as part of the ongoing DIA FME program, require proper preparation before exploitation of the weapon systems capabilities. To date, MSIC has met all the environmental requirements set forth by the DoD, U.S. Army and Redstone Arsenal. Certain environmental liabilities remain with munitions that were obtained rapidly from the short Iraq war.

### Accomplishments:

- MSIC has inventoried all FME equipment which may pose an environmental liability. This is particularly so with the large volume of equipment recently obtained from Iraq.
- MSIC has developed plans for properly disposing of all FME equipment (and/or components) which may pose an environmental liability.

## Personnel Security Investigations Program

### Description:

DIA and its Defense component customers will continue to suffer from extended PSI completion rates during the divestiture process. As an example, the OPM completion rate for "guaranteed" 75 day cases is currently running at 248 days.

### Accomplishments:

- In June 2003, DAC received OSD approval to expand the use of its contract Background Investigations Provider (BIP) through FY 04. The DIA BIP provides expeditious security investigation completion rates of 30-40 days for DIA applicant cases. Expansion of this authority will permit DAC to effectively support the current and anticipated applicant surge demands.

- DAC has also extended the use of the BIP services to cover, on a shared contract basis, a Defense component requirement for expeditious completion times.
- DAC has recently acquired several contractor assets to increase the responsiveness of its case management and control process. The accession of contractor personnel permits permanent central clearance staff to concentrate on direct adjudication support and clearance issuance.
- More frequent use is being made by DAC of its Accelerated Clearance Eligibility (ACE) procedure whereby expeditious National Agency Checks are conducted and access eligibility granted while the BIP is conducting the fast-track background investigation.

### **Real Property (Facilities) Infrastructure Program**

#### **Description:**

Failure to adopt and incorporate an active facility maintenance program could result in unreliable infrastructure that would adversely affect the mission and personnel effectiveness.

#### **Accomplishments:**

Over the last year the agency made a significant investment to enhance facility maintenance and support capital improvement projects. In addition, DIA completed an extensive recapitalization initiative that assessed the condition of all facility and support components. Each component was given a facility condition index and cataloged into a data model to provide budget forecasts and assist in scheduling the preventive maintenance and replacement of facility support assets before components reach their designed life span.

### **Contracting for Services**

#### **Description:**

An assessment of DIA's Acquisition System was completed in 2003. The assessment evaluated agency organization, policies, processes, training, tools and references that support the acquisition of supplies and services in light of best practices. Twenty recommendations and a plan of action and milestones provided a roadmap for improvement of systemic weaknesses. One recommendation that the agency implemented to improve the contracting of services is the establishment of a Component Acquisition Executive (CAE) who reports to the Deputy Director and the subsequent realignment of the Contracting Office to the Command Element reporting directly to the (CAE). Establishment of a single point of leadership is a clear signal of DIA's commitment to a strategic approach to the acquisition of services and the required enforcement of acquisition laws, policies and procedures.

#### **Accomplishment:**

To improve its intelligence support, add alternatives to deploying the right skill mix and capability to operational requirements, and correct systemic contracting weaknesses, DIA requested, and expect to receive next fiscal year, statutory authority to enter into personal services contracts. DIA would use the authority sparingly and only when the agency must carry out work for a temporary period which cannot be delayed because of a critical need; and the need cannot be met with current employees or through the direct appointment of temporary employees within the time available, and the duration of time, help is needed. For example, the authority

would be useful in support of the hunt for WMD in Iraq and similar operations in support of the Global War on Terrorism.

### Government Card Program

#### TRAVEL CHARGE CARDS

##### Description:

Delinquency and misuse can impact an individual's creditworthiness and trustfulness, which are major components when reviewing suitability for TS/SCI-level security clearances.

##### Accomplishments:

- Established points of contact in each key component (KC) to keep open-lines of communication between financial management personnel and staffers in the directorates. This ensures that problems are identified and corrected quickly.
- Prepared, analyzed and distributed the monthly delinquency report to each KC with employees who have past due accounts. Requested follow-up from each KC to explain the reason for the delinquency and steps taken to correct the problem.
- Performed data mining activities via software scans to look for suspicious activity. Sends information to IG, DAC, KC and supervisor of employee for follow-up. Disciplinary actions are taken, including removal for offenders.

#### IMPAC CHARGE CARDS

##### Description:

The Defense Intelligence Agency has placed significant emphasis on the management and controls over the IMPAC program. Annually the Inspector General focuses an audit on the IMPAC program. Recent audit reports have predominantly only noted minor problems. While the potential for the abuse exists within the program, the DIA checks and balances make it more difficult for the government to experience a significant loss without being discovered. Significant emphasis is placed on training both cardholders and billing officials on their duties, responsibilities and financial liability. DoD audits have indicated Failure of management controls also undermines the ability of the Government to seek adjustments for billing errors or fraudulent purchases that were not made by the cardholder. In addition, the failure of management controls could result in the government not obtaining the best possible price.

##### Accomplishments:

As the Agency pursues a constant improvement process with the IMPAC program, it has recognized additional controls are required to ensure all billed purchases are true and accurate. To date the effort has been to ensure adequate training and oversight is provided to both the cardholder and the billing official. Future plans include an automated reconciliation performed by downloading the bank statement and comparing the billed amount to the amount recorded for the purchase in the automated purchase register. This same solution will be used to improve the processing time required to submit for payment the IMPAC bill. Improved bill processing will enable the maximization of rebates for prompt payment. Additional training on proper use and controls for the IMPAC card program are planned for the next FY, including refresher training, and training on ensuring the government is receiving the best possible price for the goods and services received through the IMPAC program. The Agency Program Management staff has been

increased by two key positions, providing additional guidance and an internal inspection capability to the program. These actions will have a stabilizing effect on the program along with increasing the visibility of the oversight function.