Inspector General

United States

Department *of* Defense

Data Migration Strategy and Information Assurance for the Business Enterprise Information Services

		Form Approved OMB No. 0704-0188

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **30 JUL 2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE **Data Migration Strategy and Information Assurance for the Business Enterprise Information Services**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Inspector General,400 Army Navy Drive,Arlington,VA,22202**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**36**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Additional Information and Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (703) 604-8932, or by mail:

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

Acronyms and Abbreviations

ATO	Authority to Operate
BEA	Business Enterprise Architecture
BEIS	Business Enterprise Information Services
BTA	Business Transformation Agency
BTG	Business Transformation Guidance
CA	Certifying Authority
DAA	Designated Accrediting Authority
DCAS	Defense Cash Accountability System
DCD/DCW	Defense Corporate Database/Defense Corporate Warehouse
DDRS	Defense Departmental Reporting System
DFAS	Defense Finance and Accounting Service
ETP	Enterprise Transition Plan
FFMIA	Federal Financial Management Improvement Act of 1996
FMFIA	Federal Managers Financial Integrity Act of 1982
GAO	Government Accountability Office
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones

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

July 30, 2009

MEMORANDUM FOR DEPUTY CHIEF MANAGEMENT OFFICER
DIRECTOR, BUSINESS TRANSFORMATION AGENCY

SUBJECT: Data Migration Strategy and Information Assurance for the Business Enterprise
Information Services (Report No. D2009-097)

We are providing this report for review and comment. We performed this audit because DoD is
implementing the Business Enterprise Information Services (BEIS) system to consolidate
financial information and provide Enterprise-wide financial reporting. We considered
management comments on a draft of this report in preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The comments
from the Assistant Deputy Chief Management Officer were partially responsive. Therefore, we
request additional comments on Recommendations A.1., A.2., B.1., B.2., B.3., C.1., and C.2. by
August 31, 2009. See the recommendations table on page ii.

Please provide comments that conform to the requirements of DoD Directive. If possible, send
your comments in electronic format (Adobe Acrobat file only) to auddbo@dodig.mil. Copies of
your comments must contain the actual signature of the authorizing official. We cannot accept
the / Signed / symbol in place of the actual signature. If you send classified comments
electronically, you must send them over the SECRET Internet Protocol Router Network
(SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703)
601-5868 (DSN 329-5868).

Patricia A. Marsh, CPA
Assistant Inspector General
Defense Business Operations

Results in Brief: Data Migration Strategy and Information Assurance for the Business Enterprise Information Services

What We Did

We audited the Business Enterprise Information Services (BEIS) system to determine whether it had a comprehensive data migration plan, met information assurance (Federal Information Security Management Act) standards, and met the standards for the Federal Financial Management Improvement Act of 1996 (FFMIA).

What We Found

We determined that the Business Transformation Agency (BTA) internal controls were not adequate. We identified internal control weaknesses in the BTA data migration strategy, information assurance, and FFMIA compliance. Specifically, BTA did not:

- have an effective data migration strategy for Components to follow for converting legacy systems to the Business Enterprise Architecture (BEA);
- determine the sequence or schedule for when the functionality of 13 legacy systems would be transferred to BEIS;
- separate the certification and accreditation processes, thereby creating a potential conflict of interest;
- have a security plan that met Office of Management and Budget (OMB) and DoD requirements; and
- test BEIS for compliance with FFMIA.

Implementing the recommendations would improve internal controls and BEIS efforts on data migration, information security, and FFMIA compliance.

What We Recommend

We recommend that the Director, Business Transformation Agency;
- revise the Business Transformation Guidance to include a detailed, standardized methodology prescribing best practices for data migration from DoD legacy systems to the BEA structure;

- coordinate with the Defense Finance and Accounting Service (DFAS) to develop a data migration strategy identifying key milestones and a critical path for transferring the functionality of 13 legacy systems to BEIS;
- separate the roles of Certifying Authority and Designated Accrediting Authority by assigning them to two individuals;
- develop a comprehensive security plan that fulfills OMB and DoD information assurance requirements and develop procedures for testing those requirements annually;
- develop a methodology for annually reviewing the BEIS "family of systems" for compliance with FFMIA and Federal Managers Financial Integrity Act of 1982;
- assess whether the BEIS "family of systems" complies with FFMIA mandatory and technical Core Financial Management System requirements and standards; and
- develop a remediation plan for correcting any deficiencies noted.

Management Comments and Our Response

The Assistant Deputy Chief Management Officer (Assistant Deputy) responded and generally agreed with developing a data migration strategy and coordinating with DFAS on converting legacy systems functionality. The Assistant Deputy recognized the need for adhering to security guidelines, but stated DoD's position is that each program maintain its own comprehensive security plan. We request that the Assistant Deputy reconsider DoD's position on not assessing BEIS against FFMIA requirements because system change requests may have affected its compliance. We request additional comments by August 31, 2009. Please see the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Assistant Deputy Chief Management Officer	A.1., A.2., B.1., B.2., B.3., C.1., and C.2.	

Please provide comments by August 31, 2009.

Table of Contents

Introduction

We performed this audit because DoD is implementing the Business Enterprise Information Services (BEIS) system to consolidate financial information and provide Enterprise-wide[1] financial reporting. BEIS will build upon existing infrastructure to provide timely, accurate, and reliable business information from across DoD to support auditable financial statements, as well as provide detailed information for management in support of the warfighter.

Objectives

Our audit objectives were to determine whether BEIS:

- had an adequate data migration plan,

- met information assurance (Federal Information Security Management Act) standards, and

- met the standards for the Federal Financial Management Improvement Act of 1996 (FFMIA).

See Appendix A for our scope and methodology.

Background

The FY 2005 National Defense Authorization Act required DoD to develop an enterprise architecture, a transition plan, and a governance plan for business systems modernization. To accomplish these tasks, the Deputy Secretary of Defense established the Business Transformation Agency (BTA) on October 7, 2005. The BTA mission is to guide the transformation of business operations throughout DoD and to deliver Enterprise-level capabilities that meet warfighter needs. BTA also develops and facilitates the DoD-wide processes for the maintenance, refinement, approval, and implementation of the Business Enterprise Architecture (BEA).

Business Enterprise Architecture

The BEA is the DoD information infrastructure, and it includes processes, data standards, and business rules. It defines DoD's business transformation priorities, business capabilities, and the combinations of systems and initiatives that enable these capabilities. The BEA guides the evolution of DoD business capabilities Enterprise-wide and explains what DoD must do to achieve interoperable business processes. The BEA incorporates applicable laws, regulations, policies, and standards.

Enterprise Transition Plan

BTA is responsible for developing, maintaining, and executing the Enterprise Transition Plan (ETP). The ETP describes the transformation of business operations within DoD as being driven by business enterprise priorities and business capabilities. It establishes a program baseline to measure progress, and it provides DoD internal and external stakeholders with a comprehensive view of the goals, objectives, and timeframes for DoD initiatives to convert to the BEA. BTA issues the ETP in March and September annually.

---

[1] "Enterprise-wide" refers to DoD and all of its organizational entities. See the Glossary of Technical Terms at Appendix C for the definition of this and other technical terms.

Financial Management Improvement

According to the September 2008 ETP, from FY 2007 to FY 2009 DoD was to spend about $930.7 million for implementing Defense Business Transformation. Of that amount, DoD planned to spend about $132.3 million on improved financial management. The DoD strategy for improved financial management included implementing BEIS.

BEIS business objectives were to:

- create financial data that can be tracked throughout the enterprise,

- enhance and expand access to authoritative sources of financial management information for timely analysis (DoD Enterprise-level business intelligence),

- enable the linkage of resources to business outcomes,

- implement standard data elements for financial reporting, and

- eliminate existing financial management weaknesses and deficiencies.

The BEIS was based on a "family of systems" concept where existing Defense Finance and Accounting Service (DFAS) legacy financial system capabilities were transferred into the DoD enterprise financial solution. By FY 2020, BTA planned to transfer the functionality of 13 DFAS legacy systems into BEIS (see Appendix B). The BEIS current family of systems included the Defense Corporate Database/Defense Corporate Warehouse (DCD/DCW), the Defense Departmental Reporting System (DDRS), and the Defense Cash Accountability System (DCAS).

- DCD is a financial and accounting database that captures, edits, and validates the required source data, facilitates research and corrections, stores the data in a shared database, and summarizes the data at the level required for reporting. DCW contains data repositories that assist in data consolidation, standardization, and simplification and that improve the automated support provided by DCD. DCW summarizes the data required for producing standard agency-wide and departmental reports. DCW retrieves budget, accounting, and other functional data to support budget formulation, financial contract administration, cost accounting, and managerial accounting activities.

- DDRS includes three separate modules. The DDRS Audited Financial Statements module produces quarterly and annual financial statements for all of DoD. The Data Collection module captures financial data from nonfinancial feeder systems to support the financial statements and to report data from external DoD sources. The Budgetary module produces monthly and quarterly budgetary reports.

- DCAS reports expenditure data to the Treasury and includes the processing of transactions by others and transactions for others, the management of interfund and intragovernmental activity, and the performance of other Treasury and departmental functions.

Review of Internal Controls

We identified internal control weaknesses for BEIS as defined by DoD Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures," January 4, 2006. BTA did not have an effective data migration strategy because BTA transition guidance focused on Enterprise-level implementation, instead of providing the Components with sufficient detail and a standard methodology for aligning their systems to the BEA. Also, the BTA strategy lacked best

practices for data migration and its data migration schedule for BEIS was unrealistic, because BTA planned to transfer 13 DFAS legacy systems to BEIS by FY 2020, but it had not coordinated with DFAS to determine when and the sequence in which the legacy systems' functionality should transfer to BEIS (Finding A).

A potential conflict of interest existed in the BEIS information assurance certification and accreditation process, because BTA designated the same individual to serve as both Certifying Authority and Designated Accrediting Authority for the BEIS family of systems. The BEIS security plan did not meet the requirements specified by the Office of Management and Budget (OMB) and DoD (Finding B). BTA did not fully comply with financial reporting requirements of the FFMIA and the Federal Managers Financial Integrity Act of 1982 because BTA had not developed a methodology for performing a complete FFMIA assessment of the BEIS family of systems since obtaining system ownership in 2005 (Finding C).

Implementing the recommendations would improve internal controls and BEIS efforts on data migration, information security, and FFMIA compliance. We will provide a copy of the final report to the senior official responsible for internal controls at BTA.

Finding A. BTA Data Migration Strategy

BTA did not have an effective data migration strategy because its transition guidance focused on Enterprise-level implementation, instead of providing the Components with sufficient instruction and examples of a standard methodology to use for aligning their systems to the BEA structure. The guidance also lacked best practices for data migration and its data migration schedule for BEIS was unrealistic. BTA planned to transfer the functionality of 13 DFAS legacy systems to BEIS by FY 2020, but it had not coordinated with DFAS to determine when and the sequence in which the legacy systems' functionality should transfer to BEIS. Without data migration best practices, detailed instructions for a standard methodology, and examples for the Components to follow, the BTA data migration strategy jeopardized the Components' ability to deploy consistent financial management systems that could achieve BEA compliance. In addition, the lack of coordination with DFAS means that it may take 11 years for BTA to transfer legacy system functionality to BEIS and may cost the DoD $231 million. Given the rapid changes in technology, DoD's current migration plan may not support its goal of realizing financial management improvement and access to accurate, reliable information under the BEIS family of systems in a timely manner.

BTA Transition Guidance

The BTA data migration strategy was not effective because BTA transition guidance focused on the Enterprise-level implementation, did not include sufficient instruction and examples of a standard methodology for the Components to follow for converting their systems to the BEA structure, and lacked data migration best practices. BTA issued the ETP and the Business Transition Guidance (BTG) to provide needed information on converting systems to the BEA structure.

Enterprise Transition Plan

The ETP focused on the Enterprise-level implementation and lacked detailed process steps to follow for converting data from the current structure to the BEA target structure. The ETP gave DoD internal and external stakeholders an overview of the systems and initiatives that could improve business operations; however, the ETP cannot be used as a plan for data migration. Data migration is complicated because of the need to convert data from a wide variety of transactional, legacy, and third-party data sources into a new structure. Although the ETP described what DoD is trying to achieve and provided a high-level synopsis of DoD-wide goals, objectives, and proposed budget costs, it did not include a methodology for converting data and systems into a new structure. Because the BEA specified requirements for data elements, business rules, and standards, a transition plan should include a similarly detailed process for converting Component system functionality to the target structure.

Business Transformation Guidance

The Component-level instructions for implementing the BTG five-step process for the Defense Business Transformation lacked sufficient detail to provide the Components with a standard methodology for aligning their systems to the BEA. BTA issued the BTG in July 2007 to clarify roles and to establish common processes at the enterprise, Component, and program levels.

The five-step process includes:

1. setting priorities (identifying desired outcomes),
2. analyzing and approving solutions,

3. building and refining a required architecture and transition plan,
4. defining and funding the programs, and
5. executing and evaluating the business transformation.

The BTG focused on the Enterprise-level transformation, and the five-step process lacked detailed instructions for the Components to follow. For example, on the setting priorities step, the Enterprise-level instructions included a discussion of how BTA determined Enterprise-level priorities, along with a flowchart on identifying problems, mission needs, material weaknesses, unanswered questions, and desired outcomes. However, the Component and program levels did not feature those items and did not show a detailed flowchart. In addition, the BTG stated that each Component is responsible for establishing its Component-level priorities to support and complement the business enterprise priorities. Specifically, the Component instructions stated:

> Components nominate Business Enterprise Priority candidates, review them, and provide additional input to help define each Business Enterprise Priority. When Business Enterprise Priorities are identified at the DoD Enterprise level, each Component aligns the appropriate systems, standards, architectures, and plans to support achievement of Business Priority objectives.
>
> Components define Component priorities to address Component-specific mission needs or problems that either complement Business Enterprise Priorities or those not addressed by them [sic].

These instructions were not at the same level of detail as the Enterprise-level instructions. The BTG lacked clarity on how a Component would use the above instructions for aligning systems, standards, architectures, and plans to achieve the business priority objectives. In addition, the BTG stated that Components should consider:

- complexity of the need, problem, or solution,
- potential benefit of improving one or more business capabilities,
- level of risk,
- "breadth of the elements" for the perceived solution, and
- speed of capability improvement.

The BTG did not elaborate on these considerations or provide examples of how to apply them. Although the BTG provided examples of a strong and a weak business priority candidate, none of the BTG examples demonstrated the entire five-step process. Including an example that starts with the first step—setting priorities—and flows through to the last step—executing and evaluating the Business Transformation—would help the Components to apply the five-step process to their mission needs and align their systems to the BEA. Therefore, BTA should revise the BTG to include complete instructions for the Components to follow and examples that show how each of the five steps relate to each other and the listed considerations.

Data Migration Best Practices
Neither the ETP nor the BTG discussed best practices for data migration. Basic data migration best practices include identifying the data and data backup, data mapping, data cleansing, transforming the data, validating converted data, and ensuring that migrated data moved as anticipated. The ETP and BTG did not include instructions for mapping user expectations and needs, identifying data sources and targets, evaluating the data quality, analyzing gaps between the current capabilities and potential capabilities, or assessing the effort required to design, code, test, and implement the data migration at the Component level or program level. Neither the ETP nor the BTG discussed data integrity, policies, processes, procedures, controls improvements, and implementation of integrated systems. In addition, neither document

addressed information assurance standards and requirements nor how the Components should implement those standards and requirements during system conversion to the BEA structure.

Without data migration best practices, detailed instructions for a standard methodology, and examples for the Components to follow, the BTA data migration strategy jeopardized the Components' ability to deploy consistent financial management systems that can achieve BEA compliance. The Enterprise-level approach described in the ETP and BTG did not provide the guidance and support that Components needed to align their systems to the BEA. Without clear and detailed guidance for implementing data migration across DoD systems, the Components will have difficulty achieving and maintaining the high-quality data that are critical to: (1) being able to track transactions throughout the enterprise, (2) enhancing business intelligence, (3) linking resources to business outcomes, and (4) eliminating weaknesses and deficiencies. Because one of the goals of DoD is to achieve interoperable business processes, data migration should be developed and implemented in a standardized process. Therefore, we recommend that BTA revise the BTG to include a detailed, systematic, standardized methodology that would prescribe best practices for data migration, data integrity, and the overall transition into the BEA structure across DoD.

BEIS Data Migration Schedule

The BEIS data migration schedule was unrealistic because BTA planned to transfer the functionality of 13 DFAS legacy systems to BEIS by FY 2020, but it had not coordinated with DFAS to determine when and the sequence in which the legacy systems' functionality should be transferred to BEIS. The lack of coordination with DFAS means that it may take 11 years for BTA to transfer legacy system functionality to BEIS and may cost the DoD $231 million. With the rapid changes in technology, DoD may be at risk for not realizing its goals of financial management improvement and access to accurate and reliable information under the BEIS family of systems concept in a timely manner.

The ETP contained a master list of target systems and related legacy systems, along with potential migration dates. For BEIS, the ETP master list showed 13 of 15 legacy systems with a final migration date of September 30, 2020 (see Appendix B). However, the master list did not show a detailed schedule of when, during the 11 years from FY 2009 to FY 2020, the functionality of those legacy systems would transfer into BEIS. In addition, the ETP did not provide a critical path for the order in which legacy system functionality would migrate. Effective project management should include critical path techniques such as listing all activities required to complete the project, the time allowed to complete them, and related dependencies between the activities.

When asked about the transition of the 13 legacy systems' functionality into BEIS, BTA officials stated that they did not know when the transfers would occur because DFAS still owned the systems. BTA had not coordinated with DFAS to develop a detailed project plan or critical path to ensure that FY 2020 was a realistic migration completion date.

The ETP stated that for FY 2009, BTA planned to spend about $21 million on BEIS. After 11 years, assuming that the FY 2009 BEIS budget amount continued in future years, DoD could spend up to $231 million to achieve this financial management goal. According to the ETP, BEIS supports the DoD goal for financial management improvement by providing immediate access to accurate and reliable financial information, which would allow efficient and effective decision-making. Given rapidly changing technology, the lack of coordination with DFAS, and the 11-year timeline for transferring legacy system functionality, DoD is at risk for not meeting its financial management goal. By outlining dependent and related activities and reducing redundant efforts, a critical path data migration strategy may help to reduce the potential 11-year timeline and may reduce the $231 million potential cost. Therefore, we recommend that BTA

coordinate with DFAS to develop a detailed data migration strategy that identifies key milestones and a critical path for transferring the functionality of the 13 legacy systems to the BEIS family of systems.

Recommendations, Management Comments, and Our Response

During the comment period, the BTA was reorganized under the Assistant Deputy Chief Management Officer, who responded for the Department.

A. We recommend that the Director, Defense Business Transformation Agency:

1. Revise the Business Transformation Guidance to include complete instructions for the Components to follow and examples that show how the five steps relate to each other and the listed considerations. In addition, include in the revision a detailed, systematic, standardized methodology that would prescribe best practices on data migration, data integrity, and overall transition into the Business Enterprise Architecture environment across the Department of Defense.

Assistant Deputy Chief Management Officer Comments

The Assistant Deputy Chief Management Officer (Assistant Deputy) partially agreed, stating that BTA was in the process of developing a concept of operations, detailing data integrity and data migration activities, with an expected release date in 4th quarter FY 2009. However, the Assistant Deputy disagreed with revising the BTG to include data migration and data integrity activities because the intent of the BTG was not for that purpose and other documents provide that level of detail.

Our Response

The Assistant Deputy's comments are partially responsive. The Assistant Deputy comments on BTA development of a concept of operations only addressed the data migration and data integrity portion of the recommendation. Therefore, we request a listing of the documents that provide the prescribed detail. We also request additional comments on how and to what extent the concept of operations would provide instructions for the Components to follow, examples that show how the five steps relate to each other and the listed conditions, and overall transition into the BEA across DoD.

2. Coordinate with the Defense Finance and Accounting Service to develop a detailed data migration strategy that identifies key milestones and a critical path for the migration of the 13 legacy systems into the Business Enterprise Information Services.

Assistant Deputy Chief Management Officer Comments

The Assistant Deputy partially agreed that the Department should develop a detailed data migration strategy for those systems whose data would require migration to BEIS. The comments indicated that the details about whether all 13 systems would require data migration are currently under development and that once determined, the data migration strategy could be developed. The comments also indicated that BTA and DFAS are working together on this effort and would provide regular status updates, when requested.

Our Response

The Assistant Deputy's comments are partially responsive. The Assistant Deputy agreed with the need for a data migration strategy and coordination with DFAS, but indicated that

determining whether all of the systems would require data migration and developing a detailed strategy for this are under way. Therefore, we request additional comments on whether the items under development would address key milestones or a critical path for transferring the legacy system functionality into BEIS and the anticipated date for developing the data migration strategy.

Finding B. Information Assurance

A potential conflict of interest existed in the BEIS information assurance certification and accreditation process because BTA had designated the same individual to serve as both Certifying Authority (CA) and Designated Accrediting Authority (DAA) for the BEIS family of systems. Also, the BEIS security plan did not meet OMB and DoD requirements because it was not comprehensive and did not include procedures for reporting and resolving security incidents, training before granting system access, and testing for continuity of operations for the three essential systems under BEIS. As a result, the BEIS certification and accreditation authorities may have accepted undue risk when accrediting BEIS for operation.

Certification and Accreditation

A conflict of interest[2] may exist because BTA named the same individual as the CA and the DAA for the BEIS family of systems. The DAA issued an Authority to Operate (ATO) for the BEIS family of systems on November 14, 2008. An ATO is a formal notification of an accreditation decision by a DAA to accept the risk associated with operating a DoD information system. An ATO signifies that a DoD system has adequately implemented all assigned information assurance controls.

While preparing to obtain the ATO, the certification authority recommended that severity codes for 9 of the 13 reported security weaknesses listed in the July 2008 BEIS Plan of Action and Milestones (POA&M) be lowered. This was significant because system weaknesses are assigned severity codes to indicate risk level and the urgency for corrective action. Category 1 weaknesses were the most severe, and the system owner must correct them before obtaining an ATO. Category 2 weaknesses were moderately severe, and the system owner must correct them or satisfactorily mitigate them before obtaining an ATO. Category 3 were the least severe and do not prevent a DAA from issuing an ATO.

Six of the nine weaknesses were lowered from Category 2 to Category 3, and a Category 1 weakness was lowered to Category 2. The lowered Category 1 weakness indicated that the configuration control board[3] had not held regular meetings, and had not assessed subsequent system change requests for information assurance impact prior to implementation. This is significant because from FY 2006 to FY 2008, the program managers for the three essential systems for BEIS had submitted 1,209 system change requests.

An individual who serves as both the CA and the DAA, has the ability to recommend lowered category codes and then approve them, creating a lack of segregation of duties and a potential conflict of interest. The magnitude of risk increases with each system migration, and the potential migration of 13 legacy systems into BEIS represents a high level of risk (Finding A). Without regular meetings of the configuration control board to assess the information assurance impact of system change requests, the ATO's purpose of accepting the risk for system accreditation loses its significance. Therefore, BTA should appoint separate individuals to the certification and accreditation functions and positions to ensure that other missions or business

---

[2] A conflict of interest and lack of independence exist when an individual has both certifying authority and accrediting authority for the same system. Dividing duties among two or more individuals diminishes the likelihood that errors and wrongful acts could go undetected, because the activities of one individual would serve as a check on the activities of the other.

[3] The DoD configuration management process includes a configuration control board that meets regularly and implements procedures to ensure a security review and approval of all proposed DoD information system changes.

functions relying on the BEA are not compromised. In addition, BTA should ensure that the BEIS configuration control board meets regularly to review and approve all system change requests prior to implementation.

Security Planning

BTA had not developed a comprehensive plan that included procedures for reporting and resolving security incidents, training before granting system access, and testing for continuity of operations for the three essential systems under BEIS.

BTA stated that its BEIS certification and accreditation package met the requirements for a security plan. The BEIS certification and accreditation package included:

- a summary report that contained only a list of weaknesses, their corresponding control numbers, and severity;

- a System Identification Profile that listed only items such as system name, version or release number, system description, and accreditation; and

- a POA&M of listed security weaknesses.

In addition, BTA issued the BEIS Acquisition Information Assurance Strategy in June 2008. Its purpose was to provide the groundwork for integrating information assurance management into the BEIS family of systems. The strategy included a high-level discussion on the data flow from the three essential systems under BEIS.

However, neither the documents contained in the BEIS certification and accreditation package nor the BEIS Acquisition Information Assurance Strategy provided a comprehensive plan that met the requirements prescribed in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000, and DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

OMB A-130 requires agencies to ensure that information is protected at a level commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information. OMB A-130 also states that agency security plans include rules of the system, training, personnel controls, incident response capability, continuity of operations, technical security, and system interconnection. DoD Instruction 8500.2 requires that agencies implement a system security plan as part of their information assurance documentation that describes the technical, administrative, and procedural information assurance program. It must also identify specific requirements and objectives for data handling, dissemination, system redundancy, and emergency response.

Without a comprehensive security plan in place, BTA has no assurance that BEIS has a level of protection commensurate with the risk and potential magnitude of loss, misuse, or unauthorized access. In addition, the lack of segregation of duties discussed previously in this finding, combined with the request and implementation of 1,209 system changes, means that BTA may have been unaware of some BEIS risks when it issued the November 2008 ATO. Therefore, BTA should develop a comprehensive, overall security plan that meets OMB Circular A-130, Appendix III, and DoD Instruction 8500.2 requirements and develop procedures for testing those requirements annually.

Recommendations, Management Comments, and Our Response

The Assistant Deputy Chief Management Officer responded for the Department.

B. We recommend that the Director, Business Transformation Agency:

1. Separate the roles of Certifying Authority and Designated Accrediting Authority by assigning them to two individuals.

Assistant Deputy Chief Management Officer Comments

The Assistant Deputy disagreed and stated that BTA is fully compliant with DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007, which does not require the CA and the DAA to be separate individuals. In addition, the comments stated the CA and DAA resided within the Office of the Chief Information Officer and reports to a directorate that is organizationally separate from the program-level information assurance officers. The CA and DAA have no Directorate-level organizational affiliation with the system owners. In addition, because of limited staff size, there are no plans to separate the two roles at this time.

Our Response

The Assistant Deputy's comments are partially responsive. Although the Assistant Deputy cites the DIACAP as reason for having one individual perform the duties of both the CA and DAA positions, the fact that the CA/DAA resides in a different office from the system owners does not satisfy the safeguard that assigning these responsibilities to separate individuals would accomplish.

In May 2004, the National Institute of Standards and Technology issued Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems." This guide states that independence of the certification agent is an important factor in assessing the credibility of the security assessment results and ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based accreditation decision. In addition, the guide states that caution be exercised when one individual fills multiple roles in the security certification and accreditation process to ensure that the individual retains an appropriate level of independence and remains free from conflicts of interest. Because the BEIS staff member who serves as CA/DAA is able to recommend changes to the severity codes and then approve those same changes, the potential for conflict of interest exists. The lack of independence between the two positions does little to ensure a sound security posture for the information systems and diminishes the acceptable level of risk typically assumed with the issuance of the ATO. Therefore, we request that the Assistant Deputy reconsider her position and designate two individuals—one to serve as the CA and another to serve as DAA.

2. Ensure that the Business Enterprise Information Services configuration control board meets regularly to review and approve all system change requests prior to implementation.

Assistant Deputy Chief Management Officer Comments

The Assistant Deputy agreed, but did not provide any other information.

Our Response

The Assistant Deputy's comments are partially responsive. Although the Assistant Deputy agreed, the comments did not provide any further information. Therefore, we request additional comments on when the configuration control board would meet, how and to what extent they would review and approve all system change requests before implementation, and expected completion date of any procedures or policies issued.

3. Develop a comprehensive, overall security plan that meets Office of Management and Budget Circular A-130, Appendix III, and DoD Instruction 8500.2 requirements, and develop procedures for testing those requirements annually.

Assistant Deputy Chief Management Officer Comments

The Assistant Deputy disagreed, but recognized the need for strong plans for adhering to applicable security guidelines. However, the comments stated that because of the diversity of BTA's programs, the DoD's position was that having each program maintain its own set of comprehensive security documents and prepare its own exhibit to comply with OMB Circular A-130, Appendix III, was beneficial to overall security.

Our Response

The Assistant Deputy's comments are partially responsive. The Assistant Deputy comments did not state how and when comprehensive security exhibits would be prepared for DCD/DCW, DDRS, and DCAS that would comply with OMB Circular A-130, Appendix III, and DoD Instruction 8500.2 requirements. Therefore, we request additional comments on how and when the comprehensive security exhibits for those requirements are to be developed and tested.

Finding C. Financial Reporting Compliance

BTA did not fully comply with financial reporting requirements of the Federal Financial Management Improvement Act of 1996 (FFMIA) and the Federal Managers Financial Integrity Act of 1982 (FMFIA) because BTA had not developed a methodology for performing a complete FFMIA assessment of the BEIS family of systems since obtaining system ownership in 2005. As a result, BTA had no assurance that the 1,209 system change requests submitted for the BEIS family of systems do not conflict with FFMIA requirements and make its FMFIA annual Statement of Assurance inaccurate.

Compliance With FFMIA

BTA had not tested BEIS, as a family of systems, for FFMIA compliance, although BTA obtained ownership of BEIS in 2005. The FFMIA requires agencies to have financial management systems that substantially comply with the Federal financial management system requirements. The three essential systems under BEIS did not have recent tests for FFMIA compliance. For example, as the previous system owner, DFAS tested DCD/DCW in 2004 and DCAS in 2006. DFAS also tested two of the three DDRS modules: the Audited Financial Statement module (in March 2001) and the Budgetary Reporting module (in August 2002). The third module, Data Collection, was not tested.

BTA had not developed a methodology for performing a complete FFMIA compliance assessment of the BEIS family of systems. BTA stated that it planned to conduct a BEIS assessment after obtaining Milestone C approval.[4] In addition, because BTA did not have configuration control board meetings, it had no assurance that the 1,209 system change requests (Finding B) did not adversely affect BEIS compliance with FFMIA technical and administrative requirements.

OMB A-127, "Financial Management Systems," states that each agency must have an ongoing financial systems improvement planning process and perform periodic reviews of its financial systems capabilities. The "Office of Federal Financial Management: Core Financial System Requirements," January 2006, provides Federal mandatory functional and technical financial management system requirements that must be met to be compliant with Federal standards mandated by the FFMIA. Because BTA had not recently tested BEIS as a family of systems, and had not developed a methodology for conducting the tests, it had no assurance that BEIS met the FFMIA financial system requirements. Therefore, BTA should develop a methodology for implementing an annual assessment of the BEIS family of systems in accordance with FFMIA requirements.

Statement of Assurance Accuracy

BTA did not fully report internal control results as required under FMFIA. The BEIS Statement of Assurance issued on August 29, 2008, listed no material weaknesses. Section 4 of the FMFIA requires an annual statement by the agency head indicating whether the financial management systems conform to Federal financial management system requirements. FMFIA also requires that if the agency's systems do not substantially conform to financial systems requirements, the statement of assurance must report those instances and discuss the agency's plans for bringing its systems into substantial compliance. Because of the BEIS system change requests and lack of

---

[4] Achieving Milestone C means that the Milestone Decision Authority authorizes limited deployment in support of operational testing for the major acquisition information system. BEIS obtained Milestone C approval on April 29, 2009.

recent FFMIA compliance testing, the 2008 Statement of Assurance showing no material weaknesses may be inaccurate. Therefore, BTA should assess whether the BEIS family of systems complies with FFMIA mandatory and technical Core Financial Management System requirements and FMFIA standards. In addition, BTA should develop a remediation plan for correcting any deficiencies noted.

Recommendations, Management Comments, and Our Response

C. We recommend that the Director, Business Transformation Agency:

1. Develop a methodology for implementing an [annual] assessment of the Business Enterprise Information Services family of systems, in compliance with the Federal Financial Management Improvement Act of 1996 Core Financial Management System requirements.

Assistant Deputy Chief Management Officer Comments

The Assistant Deputy disagreed and stated that FFMIA does not require an annual assessment. The comments stated that BEIS is achieving FFMIA compliance in increments. DDRS and DCD/DCW achieved compliance in 2001 and 2004 respectively (Increment 1). On March 31, 2009, the Acting Defense Business Systems Acquisition Executive agreed to move DCAS to Increment II where testing for interoperability and FFMIA would occur. DCAS plans to achieve compliance before obtaining a Full Deployment Decision Review no later than first quarter 2011.

Our Response

We consider the comments partially responsive. FFMIA does not specifically require an annual assessment, but the Core Financial System Requirements implements the provisions of FFMIA and OMB A-127, "Financial Management Systems," July 23, 1993, and states that each agency must have an ongoing financial systems improvement planning process and perform periodic reviews of its financial system capabilities. Although BEIS (Increment 1) received Milestone C approval in April 2009, the Milestone C Acquisition Decision Memorandum did not address FFMIA as a necessary requirement. With the submission of 1,209 system change requests from FY 2006 through FY 2008 for the three essential systems, DDRS and DCD/DCW compliance with FFMIA may be in jeopardy.

In addition, DCAS reports expenditure data to the Treasury and includes the processing of transactions by others and for others and the performance of other Treasury and departmental functions. Waiting until 2011 to test interoperability and FFMIA compliance means that a portion of the BEIS family of systems would not achieve compliance for approximately 2 years. It is essential that DCAS be compliant with FFMIA because Fund Balance with Treasury Management is a Core Financial System Requirement. Therefore, we request that the Assistant Deputy reconsider DoD's position, and provide additional comments on currently assessing DCD/DCW and DDRS for potential noncompliance and on the DCAS testing timeframe.

2. Assess whether the Business Enterprise Information Services family of systems complies with Federal Financial Management Improvement Act of 1996 mandatory functional and technical Core Financial Management System requirements and the Federal Managers Financial Integrity Act of 1982 standards, and develop a remediation plan for correcting any deficiencies noted.

Assistant Deputy Chief Management Officer Comments

The Assistant Deputy partially agreed with the recommendation. The Assistant Deputy agreed with assessing BEIS against FFMIA requirements. However, the comments reiterated the response to recommendation C.1. on the compliance of DCD/DCW, and DDRS and the future compliance of DCAS. The comments also stated that a Management Control Matrix is submitted annually for the BEIS family of systems. In addition, the comments stated that development of a remediation plan was not required because there were no material weaknesses identified through FFMIA and FMFIA assessments.

Our Response

The Assistant Deputy's comments are partially responsive. The Assistant Deputy agreed with assessing BEIS against FFMIA requirements, but the comments appear to be in conflict. BEIS includes three essential systems, DCD/DCW, DDRS, and DCAS. However, the comments state that DCD/DCW and DDRS are FFMIA compliant and that DCAS is scheduled for testing in 2011.

FFMIA states that agencies are to implement and maintain financial management systems that comply substantially with financial management systems requirements. FMFIA requires that if the agency's systems do not substantially conform to financial systems requirements, the statement of assurance must report those instances, and discuss the agency's plans for bringing its systems into substantial compliance. One of the systems within the BEIS family of systems is not compliant, thus there should be a FFMIA assessment.

In addition, because of the 1,209 BEIS system change requests and no recent testing against the financial management system requirements, it is unclear whether there really were no material weaknesses for BEIS family of systems, and whether the 2008 Statement of Assurance was accurate. Therefore, we request additional comments on when the complete assessment for BEIS against FFMIA requirements is to occur and whether there is a need for developing a remediation plan.

Appendix A. Scope and Methodology

We conducted this performance audit from February 2008 to March 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our initial audit scope included the review of BEIS as an individual system. After discussions with the Business Transformation Agency BEIS Program Executive Officer, we learned that BEIS is a family of three separate, essential systems. Therefore, we did not evaluate BEIS enterprise level capabilities for financial reporting and we revised our scope to a review of BEIS documentation for the two remaining objectives and a review of the BTA management and oversight for the BEIS implementation and deployment. We briefed BTA management on the change of scope on April 18, 2008.

We assessed the effectiveness of information assurance documentation on the three essential systems of the Business Enterprise Information System. We inspected System Security Authorization Agreements, System Information Plans, and other relevant control documentation located at the three program management offices and the Business Transformation Agency. We interviewed the BEIS Program Executive Officer; the program managers for Defense Departmental Reporting System and the Defense Cash Accountability System; and the Enterprise Integration Office Director at the Business Transformation Agency, Arlington, Virginia. We also interviewed the DFAS Corporate Database/DFAS Corporate Warehouse program manager and the BEIS Information Assurance Officer, located in Indianapolis, Indiana.

We used the following criteria to perform this audit:

- DoD Instruction 5105.80, "Defense Business Transformation Agency (BTA)," November 12, 2008,

- DoD Instruction 8500.01E, "Information Assurance (IA),"April 23, 2007

- DoD Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures, January 4, 2006,

- DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003, and

- DoD Instruction 8500.2, "IA Implementation," February 6, 2003.

We also used the following applicable laws and regulations: the Federal Financial Management Improvement Act of 1996; the Federal Managers Financial Integrity Act of 1982; OMB Circular A-123, "Revisions to OMB Circular A-123, Management's Responsibility for Internal Control," December 21, 2004; OMB Circular A-127, "Financial Management Systems," July 23, 1993;OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 2000, and National Institute of Standards and Technology Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and the Department of Defense Inspector General (DoD IG) have issued nine reports discussing the business transformation and the BEIS. Unrestricted GAO reports can be accessed over the Internet at www.gao.gov. Unrestricted DoD IG reports can be accessed at www.dodig.mil/auditreports.

GAO

GAO Report No. GAO-09-586, "DOD Business Systems Modernization: Recent Slowdown in Institutionalizing Key Management Controls Needs to Be Addressed," May 18, 2009

GAO Report No. GAO-08-462T, "Defense Business Transformation: Sustaining Progress Requires Continuity of Leadership and an Integrated Approach," February 7, 2008

GAO Report No. GAO-07-733, "DoD Business Systems Modernization: Progress Continues to Be Made in Establishing Corporate Management Controls, but Further Steps Are Needed," May 14, 2007

GAO Report No. GAO-07-229T, "Defense Business Transformation: A Comprehensive Plan, Integrated Efforts, and Sustained Leadership Are Needed to Assure Success," November 16, 2006

GAO Report No. GAO-06-219, "DoD Business Systems Modernization: Important Progress Made in Establishing Foundational Architecture Products and Investment Management Practices, but Much Work Remains," November 23, 2005

GAO Report No. GAO-05-702, "DoD Business System Modernization: Long-standing Weaknesses in Enterprise Architecture Development Need to Be Addressed," July 22, 2005

DoD IG

DoD IG Report No. D-2007-087, "Internal Controls Over Army General Fund Transactions Processed by the Business Enterprise Information Services," April 25, 2007

DoD IG Report No. D2006-068, "Financial Management: Implementation of the Business Enterprise Information Services for the Army General Fund," March 31, 2006

DoD IG Report No. D2006-008, "Defense Departmental Reporting System and Related Financial Statement Compilation Process Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004, through March 31, 2005," October 24, 2005

Appendix B. Future BEIS System Transitions

System Name	End Migration Date	System Turn-Off Date
Collection and Expenditures Processing Reconciliation (CEPR)	To Be Determined	To Be Determined
Cash History On-Line Operator Search Engine (CHOOSE)	9/30/2020	To Be Determined
Cash Reconciliation System (CRS)	9/30/2020	To Be Determined
Departmental Financial Reporting and Reconciliation (DFRR)	9/30/2020	To Be Determined
Deposit In Transit (DIT)	9/30/2020	To Be Determined
Disbursing Returns Overseas and Afloat Activities (DRO)	9/30/2020	To Be Determined
Financial Operations Support (FOS)	9/30/2020	To Be Determined
Financial Reporting System - Accounting (FRS-Acctg)	10/30/2007	12/30/2008
Headquarters Accounting and Reporting System (HQARS)	9/30/2020	To Be Determined
International Balance of Payments (IBOP)	9/30/2020	To Be Determined
Navy Prompt Payment Interest (NPPI)	9/30/2020	To Be Determined
Check Recertification (RECERT)	9/30/2020	To Be Determined
Standard Accounting, Budgeting and Reporting System (SABRS)	9/30/2020	To Be Determined
Suspense/Aging Monitoring System (SAMS)	9/30/2020	To Be Determined
Transactions By Others (TBO)	9/30/2020	To Be Determined

Note: Although the Enterprise Transition Plan September 2008, Appendix A, shows 15 systems migrating to BEIS, only 13 of these 15 systems were to migrate by 2020.
Source: BTA, Enterprise Transition Plan, September 2008, Appendix A

Appendix C. Glossary of Technical Terms

Business Transformation Guidance. The Business Transformation Guidance provides a five-step process for transforming DoD business operations. The steps include:

1. setting priorities (identify desired outcomes),
2. analyzing and approving a solution (analyze the problem),
3. building and refining a required architecture and transition plan,
4. defining and funding the programs, and
5. executing and evaluating the business transformation

Component-level Business Transformation. Components develop strategies, schedules, and budgets for their Component Transformation, then implement these plans. Components are responsible not only for executing their individually assigned missions, but also for ensuring that joint operations run smoothly and that information flows freely across the enterprise so the DoD can function as a cohesive whole.

Configuration Management. The DoD configuration management process includes requirements for formally documenting configuration management responsibilities; a configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes; a testing process to verify proposed configuration changes prior to implementation; and a verification process to provide additional assurance that the configuration process is working effectively and that changes outside the process are technically or procedurally not permitted.

Data migration. The process of translating data from one format to another and may involve the restructuring of data by merging fields or changing formats. Data migration transforms data from a variety of transactional, legacy, current, and historical data sources into a new representation of the data. This requires the data to be:

- profiled and extracted from current systems,
- cleansed of incorrect, redundant or outdated records,
- transformed into the new data representations,
- tested to ensure that the data migrated correctly, and
- loaded into the new application environment.

Defense Acquisition System. According to DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003, Milestone C authorizes entry into deployment in support of operational testing for major acquisition information systems. The Milestone Decision Authority commits DoD to production at Milestone C.

Designated Accrediting Authority. The official with the authority to assume formal responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Approving Authority and Delegated Accrediting Authority.

DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system applications, enclaves, outsourced information technology-based processes, and platform interconnections.

Enterprise. Refers to the Department of Defense, including all of its organizational entities.

Enterprise Architecture. A management practice for aligning resources to improve business performance and help agencies execute their core missions. An enterprise architecture describes the current and future state of the agency, and lays out a plan for transitioning from the current state to the desired future state.

Enterprise-level Transformation. This includes data standards, business rules, specific systems, and an associated integration layer of interfaces for the Components. These standards are established through cooperation and represent the "rules of engagement" to which all DoD Components must adhere. Thus, while the Department is not dictating how to transform, it is ensuring that each Component's transformational program increases the Department's ability to reap the benefits of improved information exchange across organizational boundaries. This type of integration will drive the Department down the path to interoperability and accelerate the Services' transformation efforts.

Information Assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance Certification and Accreditation. The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.

Information Assurance Control. An objective information assurance condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities expressed in a specified format (such as a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality.

Milestone C. Achieving Milestone C means that the Milestone Decision Authority authorizes entry into limited deployment in support of operational testing for the major acquisition information system.

Tiered Accountability. DoD implemented tiered accountability for accomplishing the overall business transformation. It requires each tier in the DoD organizational hierarchy to focus on only those requirements that are relevant for that specific tier. The three accountability tiers are:

   Enterprise Level. At the Enterprise tier, the Defense Business Systems Management Council, the Principal Staff Assistants, and the Business Transformation Agency work with the Components to create architectures, develop plans, make decisions, and manage the execution of DoD-wide business capability improvements.

   Component Level. The Components are responsible for developing and maintaining their architecture transition plans, cost and schedule data, and performance data that should detail their priorities and integration with the Business Enterprise Architecture and the Enterprise Transition Plan. The Components are charged as pre-certification authorities for performing the necessary due diligence that would ensure compliance is achieved and certifies achievement during the annual investment review process and at appropriate milestone decision points.

   Program Level. Program managers and program executive officers ensure program information is current, complete, and accurate. They are responsible for developing the program transition plan that integrates with transition plans at the enterprise and Component levels.

Management Comments

Assistant Deputy Chief Management Officer Comments

OFFICE OF DEPUTY CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

MAY -7 2009

Ms. Holly Williams
Program Director
Automated Financial Systems Division
Defense Business Operations
Department of Defense Office of Inspector General
400 Army Navy Drive
Arlington, VA 22202-4704

Dear Ms. Williams:

This is the Department of Defense (DoD) response to the DoD Inspector General (IG) draft report on the "Data Migration Strategy and Information Assurance for the Business Enterprise Information Services (BEIS)," dated March 23, 2009 (Project No. D2008-D000FB-0120.000).

Of the seven recommendations issued, the Department concurs with one (B.2), partially concurs with three (A.1, A.2, and C.2) and non-concurs with three (B.1, B.3, and C.1). On recommendations with a partial concurrence, either the Department agrees in principle with the intent of the recommendation, but has chosen an alternative path for implementing the recommendation or part of the recommendation may not be applicable. On recommendations with a non-concurrence, existing federal or DoD policies do not require the recommended action.

The Department appreciates the DoD IG's assessment of the BEIS family of systems, and we will continue to evaluate the program's data migration and information assurance to identify areas for continued improvement. As the Department continues to move forward, we welcome the DoD IG's insight and participation in our on-going defense business transformation efforts.

Elizabeth A. McGrath
Assistant Deputy Chief Management Officer

RECOMMENDATION A.1: We recommend that the Director, Business Transformation Agency (BTA) revise the Business Transformation Guidance (BTG) to include complete instruction for the Components to follow and examples that show how the five steps relate to each other and the listed considerations. In addition, include in the revision a detailed, systematic, standardized methodology that would prescribe best practices on data migration, data integrity, and overall transition into the Business Enterprise Architecture (BEA) environment across the Department of Defense (DoD)

DOD RESPONSE: Partially Concur.

The Department recognizes the need for further guidance concerning data integrity and data migration. The BTA is in the process of developing a Concept of Operations that details these activities, with an expected release date of 4th quarter FY09.

However, the Department does not concur with including such additions in the BTG because the document is not intended to provide the level of detail that the DoD IG is prescribing. Per page 6 of the BTG, "The intent of this guidance is to: 1) Frame the overall Defense Business Transformation Approach; 2) Clarify roles of participants; 3) Establish common processes to govern, manage, plan, and execute business transformation at all levels; [and] 4) Describe required architecture and planning information. BTG does not provide detailed, step-by-step procedures for developing architecture products, transition plan products, or program acquisition documentation. Each of these products has its own governing documents that provide this detail."

RECOMMENDATION A.2: We recommend that the Director, Business Transformation Agency coordinate with the Defense Finance and Accounting Service (DFAS) to develop a detailed data migration strategy that identifies key milestones and a critical path for the migration of the 13 legacy systems into the Business Enterprise Information Services (BEIS).

DOD RESPONSE: Partially Concur.

For those systems whose data will require migration to BEIS, the Department concurs with the recommendation to develop a detailed data migration strategy. However, details regarding whether all 13 systems will require data migration are currently under development. Once determined, the data migration strategy for the systems that will require migration can be developed. DFAS and BTA are

Page 1 of 4

22

committed to working together on this effort and upon request will provide regular status updates.

RECOMMENDATION B.1 We recommend that the Director, Business Transformation Agency separate the roles of Certifying Authority (CA) and Designated Accrediting Authority (DAA) by assigning them to two individuals.

DOD RESPONSE: Non-Concur.

The BTA is fully compliant with the DoD Information Assurance Certification and Accreditation Process (DIACAP) regulations as stipulated in DoD Instruction 8510.01, which does not require the CA and DAA to be separate individuals.

The BTA recognizes the need to protect the security of the Agency's systems by separating information assurance roles and responsibilities and maintaining appropriate checks and balances. The CA/DAA, who resides within the Office of the Chief Information Officer (OCIO), reports to a Directorate that is organizationally separate from the Directorates that the program level information assurance officers are assigned under. Therefore, the CA/DAA has no Directorate-level organizational affiliation with the system owners. Additionally, due to limited staff size within the OCIO, there are no plans to separate the CA and DAA roles at this time.

RECOMMENDATION B.2: We recommend that the Director, Business Transformation Agency ensure that the BEIS configuration control board meets regularly to review and approve all system change requests prior to implementation.

DOD RESPONSE: Concur.

RECOMMENDATION B.3: We recommend that the Director, Business Transformation Agency develop a comprehensive, overall security plan that meets Office of Management (OMB) Circular A-130, Appendix III, and DoD Instruction 8500.2 requirements, and develop procedures for testing those requirements annually.

DOD RESPONSE: Non-Concur.

The BTA recognizes the need for strong plans to ensure adherence with applicable security guidelines. However, due to the diverse nature of the BTA's programs, it is the Department's position that it is more beneficial overall security to have the

programs maintain their own set of comprehensive security documents. Each program will prepare its own exhibit to comply with OMB Circular A-130, Appendix III.

RECOMMENDATION C.1: We recommend that the Director, Business Transformation Agency develop a methodology for implementing an annual assessment of the BEIS family of systems, in compliance with the Federal Financial Management Improvement Act (FFMIA) of 1996 Core Financial Management System requirements.

DOD RESPONSE: Non-Concur

The FFMIA of 1996 does not require an annual assessment.

BEIS FFMIA compliancy is being achieved in increments. Increment I, which includes the Defense Departmental Reporting System (DDRS) and Defense Corporate Database/Defense Corporate Warehouse (DCD/DCW), achieved compliance in 2001 and 2004, respectively. Increment II, which includes the Defense Cash Accountability System (DCAS), will achieve compliance prior to obtaining a Full Deployment Decision Review, estimated no later than 1st quarter FY11. The Acting DBSAE has approved this plan per the attached memorandum (Attachment A).

RECOMMENDATION C.2: We recommend that the Director, Business Transformation Agency assess whether the BEIS family of systems complies with FFMIA of 1996 mandatory functional and technical Core Financial Management System requirements and the Federal Managers Financial Integrity Act (FMFIA) of 1982 standards, and develop a remediation plan for correcting any deficiencies noted.

DOD RESPONSE: Partially Concur.

The Department concurs with the requirement to assess BEIS against FFMIA requirements. As stated in the Department's response for Recommendation C.1, Increment I (DDRS, DCD/DCW) compliance was achieved in 2001 and 2004, respectively, to ensure that it substantially conformed to financial systems requirements. Increment II (DCAS) compliance will be achieved prior to obtaining a Full Deployment Decision Review for this increment. Additionally, a Management Control Matrix has been submitted for the BEIS Family of Systems on an annual basis since 2006.

Page 3 of 4

However, because there have been no material weaknesses identified through the
FFMIA and FMFIA assessments, development of a remediation plan is not
currently required.

BUSINESS TRANSFORMATION AGENCY
1851 SOUTH BELL STREET
ARLINGTON, VA 22202

31 MARCH 09

MEMORANDUM

THRU PROGRAM EXECUTIVE OFFICER ENTERPRISE FINANCE

FOR BUSINESS ENTERPRISE INFORMATION SERVICES PROGRAM MANAGER

SUBJECT: Approval of Business Enterprise Information Services (BEIS) Family of Systems (FoS) Federal Financial Management Improvement Act (FFMIA) Certification Plan for Increment I

I approve the Business Enterprise Information Services (BEIS) Family of Systems (FoS) Increment I plan for Federal Financial Management Improvement Act (FFMIA) Certification based on documentation presented.

I agree that both elements of BEIS FoS Increment I, Defense Departmental Reporting System (DDRS) and DFAS Corporate Database/DFAS Corporate Warehouse (DCD/DCW), met the certification requirements stated in the FFMIA of 1996 (Public Law 104-208) and have determined the existing approved FFMIA certification packages for both DCD/DCW and DDRS satisfy the FFMIA certification for BEIS FoS Increment I.

I also concur with the BEIS PM recommendation to move the Defense Cash Accountability System (DCAS) portion of the BEIS FoS in its entirety to Increment II where it will undergo the required Interoperability (IOP) and FFMIA/FFMR validations.

My point of contact for this issue is Mr. Tracy Tynan

Keith E. Seaman
Acting Director, Defense Business Systems
Acquisition Executive
Business Transformation Agency

Inspector General
Department *of* Defense