Defense Finance and Accounting Service

DFAS 7900.4-M
Financial Management Systems Requirements Manual
Appendix 5, Guidance on FFMIA

September 2011

Financial Management Center of Excellence

Appendix 5

Guidance on FFMIA Compliance, Evaluation, and Reporting

From

OMB Circular A – 127

And

DoDFMR Volume 1, Chapter 3

TABLE OF CONTENTS

OMB Circular A-127 (Jan 2009)

1. Purpose

The Office of Management and Budget (OMB) Circular No. A-127 (hereafter referred to as Circular A-127) prescribes policies and standards for executive departments and agencies to follow concerning their financial management systems.

2. Rescission

This Circular supersedes all previously issued versions dated July 23, 1993, June 10, 1999, and December 1, 2004.

3. Authorities

This Circular is issued pursuant to the Chief Financial Officers Act (CFO Act) of 1990, P.L. 101-576; the Federal Managers' Financial Integrity Act (FMFIA) of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.); 31 U.S.C. Chapter 11; and the Federal Financial Management Improvement Act (FFMIA) of 1996, P.L. 104-208 (31 U.S.C. 3512 et seq.).

4. Applicability/Scope

A. The policies in this Circular apply to the financial management systems of all agencies in the executive branch of the government, including any executive department, military department, independent agency, government corporation, government controlled corporation, or other establishment. Agencies not included in the CFO Act are exempted from certain requirements as noted in Section 8 and Section 9.

B. The financial management systems identified in Section 5 are subject to the policies contained in OMB Circular No. A-130, "Management of Federal Information Resources" (hereafter referred to as Circular A-130).

C. The financial management systems identified in Section 5 must adhere to the policies and procedures contained in OMB Circular No. A-123, "Management's Responsibility for Internal Control" (hereafter referred to as Circular A-123).

5. Definitions

For the purposes of this Circular, the following definitions apply:

A financial system, hereafter referred to as a core financial system, is an information system that may perform all financial functions[1] including general ledger management, funds management, payment management, receivable management, and cost management. The core financial system is the system of record that maintains all transactions resulting from

[1] See Core Systems Functions from the Financial Systems Integration Office (FSIO) *Core Financial System Requirements*

financial events. It may be integrated through a common database or interfaced electronically to meet defined data and processing requirements. The core financial system is specifically used for collecting, processing, maintaining, transmitting, and reporting data regarding financial events. Other uses include supporting financial planning, budgeting activities, and preparing financial statements. Any data transfers to the core financial system must be: traceable to the transaction source; posted to the core financial system in accordance with applicable guidance from the Federal Accounting Standards Advisory Board (FASAB); and in the data format of the core financial system.

A mixed system (often referred to as a feeder system) is an information system that can support both financial and non-financial functions.

A financial management system includes the core financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, and controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. The following are examples of financial management systems: core financial systems, procurement systems, loan systems, grants systems, payroll systems, budget formulation systems, billing systems, and travel systems.

A financial event is any activity having financial consequences to the Federal government related to the receipt of appropriations or other financial resources; acquisition of goods or services; payments or collections; recognition of guarantees, benefits to be provided, or other potential liabilities; distribution of grants; or other reportable financial activities.

6. Policy

A. FSIO Certified Commercial System

Agencies must use a core financial system that is a commercial off-the-shelf (COTS) system and has been certified by the Financial Systems Integration Office (FSIO) as meeting the core financial system requirements. If the core financial system is not up-to-date with FSIO certification, agencies should consider upgrading to a certified version of the same COTS product or implement a different certified product.

B. FSIO Testing

FSIO will establish processes for testing COTS software products supporting core financial system requirements. The test will verify that the COTS products meet the core financial system requirements. The product configuration used in the test will become the certified configuration for that software product.

C. Frequency of FSIO Testing

The FSIO certification tests are to be conducted as prescribed in the Core Federal Financial System Software Qualification Testing Policy issued by FSIO.

D. Policy Exceptions

In general, agencies will not be exempt from any part of the policy. However, there may be two exceptions given a legitimate need: (1) deviation from the standard configurations (see Section 6.E; and (2) exception to competition when upgrading or modernizing core financial systems (see Section 7.D).

E. Standard Configuration
Agencies must utilize the certified configurations as defined, tested and certified by FSIO as they become available. However, exceptions may be granted if there is a legitimate and valid need for them. To obtain an exception to deviate from the certified configurations, OMB must first be provided with a justification for approval. Agencies will be required to register any approved configuration changes with FSIO. FSIO will issue guidance, as needed, with respect to implementing the certified configurations and requesting and reporting deviations.

F. Periodic Review of Standard Configuration
Agencies that have implemented core financial systems with the certified configurations will undergo periodic reviews which will be performed by FSIO. The reviews will assess whether deviations occurred from the certified version. FSIO will issue guidance with respect to these periodic reviews.

G. Adoption of Standard Business Processes
Agencies are required to adopt the standard government business processes[2] as established by FSIO. These standards will be included in the FSIO's core financial system requirements documentation. The standards should be adopted as agencies upgrade to the next major release of their current core financial system or migrate to a different core financial system.

H. Implementation
During implementation, agencies must monitor the project's progress and institute performance measures[3] to ensure that it is on schedule and within budget. Agencies must also assess risks regularly and mitigate them in a timely manner. To do so, agencies must provide periodic briefings to OMB, at its request, that detail the project's progress.

I. Maintenance
Agencies must ensure that their service provider periodically performs on-going maintenance of the core financial system to support the most current Federal business practices and systems requirements. Agencies must also verify whether their service provider is continuing to meet its Service Level Agreement.

J. Continuity of Operation Plan (COOP) and Disaster Recover (DR) Plan

[2] The standard business processes are defined by FSIO in *the Standard Federal Financial Business Processes (SFFBP) Document*
[3] See OMB Memorandum M-05-23, Improving Information Technology (IT) Project Planning and Execution

Agencies must continually evaluate that their core financial systems' Continuity of Operation Plan and Disaster Recovery Plan are both adequate and feasible. The plan shall be tested on an annual basis.

K. Documentation

Core financial systems' processing instructions shall be clearly documented in hard copy or electronically in accordance with (a) the requirements contained in the core financial system requirements document issued by FSIO or (b) other applicable requirements. All documentation (e.g., software, system, operations, user manuals, and operating procedures) shall be kept up-to-date and be readily available for examination. System user documentation shall be in sufficient detail to permit a person with knowledge of the agency's programs and of systems generally, to obtain a comprehensive understanding of the entire operation of each system. Technical systems documentation such as systems specifications and operating instructions shall be adequate to enable technical personnel to operate the system in an effective and efficient manner.

L. Training and User Support

Adequate training and appropriate user support shall be provided to the users of the core financial systems, based on the level, responsibility, and roles of individual users. Training shall enable the users of the systems at all levels to understand, operate, and maintain the system.

M. Core Financial System Requirements Title Change

The core financial system requirements document previously issued under the Office of Federal Financial Management (OFFM) will be considered to have been issued under the Financial Systems Integration Office (FSIO).

N. Non-Core Financial System Requirements

Specific non-core financial system requirements, previously published by the Joint Financial Management Improvement Program (JFMIP) and known as the JFMIP Federal Financial Management System Requirements (FFMSR) series, should be regarded as guidance when defining system requirements for acquisition. The FFMSR requirements are not part of the Federal financial management systems requirements for FFMIA and therefore should not be used to determine substantial compliance.

7. Service Provider Requirements

A. Use of External Providers

When upgrading to the next major release of its current core financial system or modernizing to a different core financial system, an agency must use an external provider which is either a Federal shared service provider that has been designated by OMB or a commercial vendor. The implemented system must also be maintained by the external provider. If agencies cannot migrate to an external provider immediately, then they should take incremental steps by moving their hosting or application management support to a provider.

B. Minimum Requirements of External Providers
The external provider must demonstrate to the Federal agency its ability to:

1) Meet applicable Federal requirements, (e.g., the Federal Information Security Management Act of 2002 (FISMA) and compliance with Section 508 of the Rehabilitation Act and FFMIA);

2) Operate and maintain a COTS software package that complies with FSIO's core financial system requirements;

3) Meet the requirements of the Financial Management Due Diligence Checklist; and

4) Provide a SAS 70 audit report to its customers or allow customer auditors to perform appropriate tests of internal controls at its organization.

FSIO will maintain and publish the most current list of OMB designated Federal service providers and the Due Diligence Checklist.

C. Competitive Process
Agencies are required to hold a competition among the OMB designated Federal providers and commercial vendors when upgrading their current core financial system or modernizing to a different core financial system.

D. Competition Exemption
Agencies may be allowed to conduct a non-competitive migration or a competitive migration involving only commercial providers (if authorized by law) or OMB designated providers if they prepare a full justification, generally including the type of information called for by section 6.303-2 of the Federal Acquisition Regulation (FAR). The justification shall be approved by the agency's Chief Financial Officer, Chief Information Officer, and Chief Acquisition officer. Agencies shall confer with OMB prior to proceeding with a migration that is noncompetitive or is otherwise limited in accordance with this paragraph.
An agency may rely on its in-house operations if the agency demonstrates to OMB that its internal operations represent a best value and lower risk alternative. This demonstration shall be made through the establishment of a most efficient organization and public-private competition, unless there is a justified basis for foregoing competition or for using a limited form of competition, such as public-public competition. The justification shall be documented in the same general manner prescribed in Part 6 of the FAR for the use of other than full and open competition.

E. Tracking Results
Agencies shall monitor performance, regardless of the selected service provider, for all performance periods stated in the solicitation. Performance measurement and reporting shall be consistent with OMB guidance on earned value management. See OMB Memorandum M-05-23.

8. FFMIA Compliance

A. Definition of Substantial Compliance

Substantial compliance is achieved when an agency's financial management systems routinely provide reliable and timely financial information for managing day-to-day operations as well as to produce reliable financial statements, maintain effective internal control, and comply with legal and regulatory requirements. FFMIA substantial compliance will be determined annually at the department-wide or agency-wide level for the 24 major CFO Act agencies.[4] Agencies can determine whether the requirements are being met by applying the FFMIA risk model, which ranks risks from nominal to significant (See Figure 1). The risk indicators in the model assist agencies in determining whether reliable and consistent information is available for decision making. The higher the risk, the more likely the agency is non-compliant.

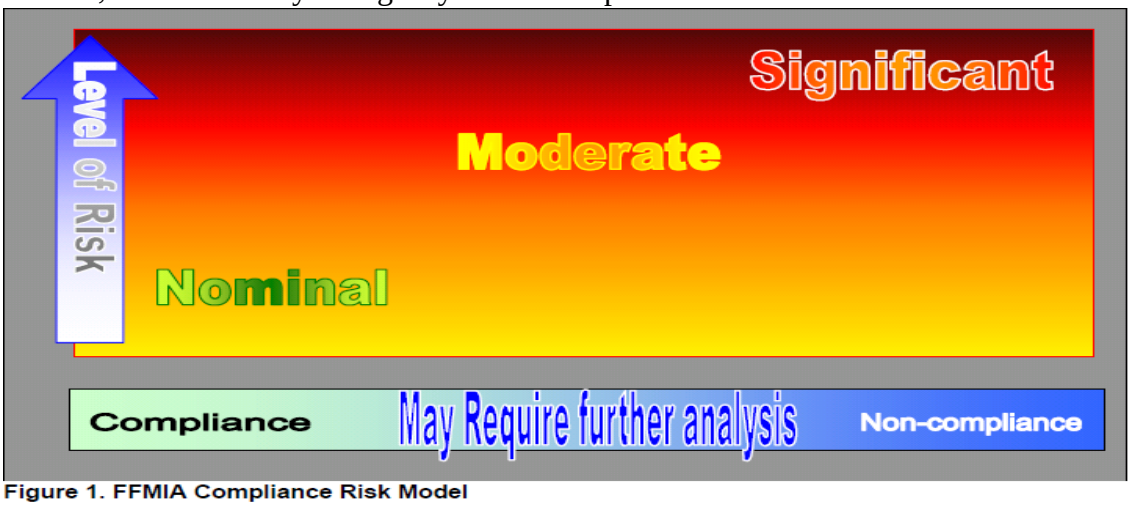

Figure 1. FFMIA Compliance Risk Model

If agencies fall under a nominal risk category, then the risk of noncompliance is low. Meeting the indicators for nominal risk signals that substantial compliance is adequately supported and additional supporting information should not be necessary. However, during the course of its financial statements audit, the financial statement auditor may request additional information to support compliance or, at its discretion, perform further testing. If agencies are under a significant risk category, then they are not in compliance with FFMIA and must identify remediation plans and resolve them. Agencies under moderate risk may need to provide further information to support compliance. Specific guidance may be found in the FFMIA Implementation Guide of 2008.[5]

---

[4] The 24 CFO Act agencies are defined in Appendix A of the OMB Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended.

[5] http://www.whitehouse.gov/omb/financial/ffmia_implementation_guidance.pdf

B. FFMIA Risk Indicators

Table 1 provides key indicators within each of the three risk categories for determining the level of risk for each agency. The indicators represent the major criteria for determining FFMIA compliance, but may not reflect indicators that would be unique to specific agency missions.

Risk Category	Indicators	FFMIA Determination
Nominal Risk	1. FSIO certified system; 2. No internal control findings reported under Section 2 FMFIA over financial reporting and Section 4; 3. No FISMA significant deficiencies impacting financial management systems; 4. Unqualified audit opinion; 5. No auditor-reported material weakness; 6. No persistent[7] auditor-reported significant deficiencies related to financial management systems; and 7. No significant manual year-end adjustments both in number of entries and value of transactions.	Substantial compliance may be determined without additional supporting information
Moderate Risk	1. Non-FSIO certified system; 2. Internal control findings reported under Section 2 FMFIA 3. Qualified audit opinion; 4. Auditor-reported material weakness; 5. Persistent auditor-reported significant deficiencies related to financial management systems; or 6. Significant manual year-end adjustments both in number of entries and value of transactions.	Substantial compliance only if agencies provide additional information to demonstrate compliance
Significant Risk	1. Findings reported under FMFIA Section 4; 2. FISMA significant deficiencies impacting financial management systems; or 3. Disclaimer or adverse opinion.	Noncompliance

Table 1

Note: Footnote 7 in Table 1 refers to auditor-reported significant deficiencies lasting 3 or more years

C. Section 803(a) Requirements

1) Federal Financial Management System Requirements

The Federal Financial management system requirements consist of three parts: (1) computer security requirements; (2) internal controls; and (3) FSIO core financial system requirements.

a. Computer Security Requirements
The security controls requirements are defined by FISMA and Circular A-130 and/or successor documents.

b. Internal Controls
The internal controls requirements are internal control objectives of Circular A-123 (including the body of the A-123 and Appendix A), which ensure resource use is consistent with laws, regulations, and policies; resources are safeguarded against waste, loss, and misuse; and reliable data are obtained, maintained, and disclosed in reports.

c. FSIO Core Financial System Requirements
The core financial system requirements are defined by FSIO's core financial system requirements.

2) Federal Accounting Standards
When applicable, agency financial management systems shall maintain accounting data to permit reporting in accordance with Federal accounting standards, and reporting requirements issued by the Director of OMB and/or the Secretary of the Treasury. Where no accounting standards have been recommended by FASAB and issued by the Director of OMB, the systems shall maintain data in accordance with the applicable accounting standards used by the agency for preparation of its financial statements.

3) Application of the U.S. Government Standard General Ledger at the Transaction Level
Financial events shall be recorded applying the requirements of the U.S. Government Standard General Ledger (USSGL). Application of the USSGL at the transaction level means that each time an approved transaction is recorded in the system, it will generate appropriate general ledger accounts for posting the transaction according to the rules defined in the USSGL guidance.

D. Applicability of FFMIA
Agencies covered by the CFO Act must comply with the FFMIA Section 803(a) requirements. Agencies not covered under the Act are not required to comply with the FFMIA requirements, but are still encouraged to adhere to them.

The FFMIA law requires all financial management systems to adhere to FFMIA Section 803(a) requirements. However, certain Section 803(a) requirements will only be applicable to the core financial system. All systems must be in compliance with computer security and internal controls requirements. However, only core financial systems must

be compliant with FSIO core financial system requirements and accounting standards as well as apply the USSGL at the transaction level. The core system requirements do not apply to mixed systems unless the systems perform the core system function. Additionally, mixed systems should only adhere to the specific accounting standards that are applicable to mixed systems (e.g., loans). Finally, mixed systems do not have to record transactions using USSGL accounts. Nonetheless, data coming from the mixed system must be posted to the core financial system using proper USSGL accounts and accounting standards.

E. Review of Financial Management Systems

Agencies should perform an annual review of their financial management systems to verify compliance with computer security and internal controls. When reviewing their systems, agencies should leverage the results of related reviews such as those required by FISMA and Circular A-123. In general, agencies using the latest FSIO certified financial system are not required to perform a separate review of their core financial system to verity compliance with the FSIO core financial systems requirements, accounting standards, or USSGL. Agencies that do not use the latest version of the FSIO certified system may be required to perform self assessments of their core financial system.

9. Assignment of Responsibilities

A. Agency Responsibilities

Agencies shall perform the financial management system responsibilities prescribed by legislation referenced in Section 3 "Authorities" of this Circular. In addition, each agency shall take the following actions:

1) Oversight of Financial Management Systems

Agencies are responsible for managing their financial management systems even when they utilize a service provider to implement, operate and maintain the systems. Agencies must also ensure that their financial management systems meet applicable Federal requirements and are adequately supported throughout the systems' life cycle. All agreement and contracts with service providers must clearly outline the goals necessary to achieve sound financial management. Furthermore, agencies must monitor the service providers' performance and ensure that service failures are resolved promptly.

2) Develop and Maintain Agency-wide Financial Management System Plans

Agencies must prepare a plan for their financial management systems, which incorporates their strategic plan, financial management plan, enterprise architecture, and budget request. Once a plan is established, it must be updated at least annually or earlier when a significant event occurs (e.g., reorganization).

In establishing a plan, an agency must consider its own financial management systems' life cycle. Specifically, it must project a reasonable useful life of the investment and plan the next system upgrade accordingly. Technology trends and

product support schedules should be considered when projecting the useful life. The plan must also identify existing problems related to the current system.
Each financial management system plan must:

a. describe the existing financial management system architecture and any changes needed to implement a targeted architecture;
b. be consistent with the enterprise architecture, information resource management plan, and IT capital plan;
c. provide a strategy for maintaining adequacy, consistency, and timeliness of financial information;
d. identify projects necessary to achieve FFMIA substantial compliance within three years from the date of noncompliance;
e. contain milestones for correcting any material weaknesses;
f. identify and make proposals to eliminate duplicative and unnecessary systems;
g. include a strategy to migrate to an external provider;
h. contain milestones for equipment acquisitions and other actions necessary to implement the plan;
i. identify financial management personnel needs and actions to ensure those needs are met; and
j. estimate the costs of implementing the plan.

Once a plan is established, an agency must obtain approval from its Investment Review Board (IRB) if major changes are needed. The approved financial management systems plan will provide a basis for the agency's business case. The business case must include an estimate of the full cost necessary to complete the upgrade, and have considered different alternatives in measuring the risks and costs for the plan. The business case will be used to justify funding and, therefore, must be clearly stated in the agency's budget request. Agencies should communicate progress against the approved business case and financial management systems plan with OMB throughout the financial management system lifecycle.

A summary of the plan should be included in the agency's annual financial report as instructed in OMB Circular No A-136, "Financial Reporting Requirements." For agencies not covered under the CFO Act, they need to prepare the plans but are not required to report them in their annual financial reports.

3) Develop and Maintain an Agency-wide Inventory of Financial Management Systems
Agencies are required to maintain an inventory of their existing and proposed financial management systems. Annually, agencies will provide FSIO with an annual inventory of their financial management systems.

4) Develop and Maintain Agency Financial Management System Directives

Agencies shall issue, update, and maintain agency-wide financial management system directives to reflect policies defined in this Circular.

B. FSIO Responsibilities

FSIO will issue and maintain all financial management business processes standards, core financial system requirements documents and all software certifications. Additionally, FSIO will develop and administer the certification test; notify the public and agencies when a software package successfully completes the certification test; and provide interested parties with information on the results of the certification tests for certified software products.

C. GSA Responsibilities

GSA will make procurement vehicles available to agencies for acquiring software that has been certified according to the processes in Section 6.B.

10. Information Contact

All questions or inquiries should be referred to the OFFM Financial Analysis and Systems Branch at (202) 395-3993.

11. Review Date

This Circular shall be reviewed three years from its issuance date to ascertain its effectiveness.

12. Effective Date

This Circular is effective as of October 1, 2009. However, early implementation, where applicable, is encouraged.

DODFMR VOLUME 1, CHAPTER 3 (Oct 2008)
FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT OF 1996
COMPLIANCE, EVALUATION, AND REPORTING

0301 PURPOSE AND AUTHORITATIVE GUIDANCE

As outlined in this chapter, the DoD policy applicable to achieving FFMIA compliance and structure is consistent with OMB Circular A-127 and reflects guidelines to aid DoD entities in achieving compliance with the FFMIA in the period before auditability.

This chapter defines and prescribes the following:

A. Integrated Financial Management Systems (IFMS).
B. FFMIA compliance, to include timeframes when target IFMS and Financial Systems must be evaluated for FFMIA compliance; how (and by whom) target IFMS and Financial Systems are evaluated and tested for FFMIA compliance; and how and when compliance is reported, measured, and monitored.
C. Applicability (Reporting Entities for FFMIA purposes).
D. Criteria for determining which financial and mixed systems must be evaluated for FFMIA compliance.
E. Requirements for developing, maintaining, and executing remediation plans when a Department of Defense (DoD) Component is not in compliance with FFMIA.
F. Roles and responsibilities of the Office of the Secretary of Under Secretary of Defense (Comptroller) (OUSD (C)) and DoD Components.

0302 BACKGROUND

The FFMIA provides the basis for the development and implementation of financial systems (to include mixed systems) that provide reliable financial management information. The intent of this Act is to provide standard guidance for Federal Agencies to follow in developing usable systems that support federal manager responsibilities to:

A. Provide reliable and timely financial information for managing current operations,
B. Prepare financial statements and other required financial and budget reports, and
C. Account for their assets reliably, in order to protect them from loss, misappropriation, or destruction.

FFMIA compliance is measured at the Reporting Entity level and requires:

A. Annual assessments reported by the Agency/Entity Head.
B. Formal remediation plans when IFMS or financial systems fail to comply.

C. Assessments by auditors during financial statement audits.

0303 DOD POLICY

The DoD approach to FFMIA compliance capitalizes on the related efforts to achieve auditability and to maintain effective internal controls over financial reporting (ICOFR). These related efforts, guided by OMB Circular 123 (Management's Responsibility for Internal Controls) and OMB Circular 136 (Financial Reporting Requirements), strive to achieve many of the same objectives as the objectives of the FFMIA. As a result, much of the documentation and testing in support of the auditability and ICOFR also supports the Department's efforts to become FFMIA compliant.

The following defines the FFMIA compliance approach in order to help ensure that the Department addresses these related requirements efficiently:

A. Reporting Entities

All DoD Components must adhere to the FFMIA and OMB Circular A-127 requirements. All DoD Reporting Entities listed in Volume 6B, Chapter 1, paragraphs 010601, 010602, and 010605 of this Regulation are directed to report their compliance with FFMIA as part of their Annual Statement of Assurance beginning in fiscal year 2010, as required by the Federal Managers Financial Integrity Act and guidance issued annually by the OUSD(C). The FFMIA compliance of individual financial and mixed systems are also to be identified in the DoD Information Technology Portfolio Repository (DITPR) as part of the annual review process for Defense business systems undertaken in accordance with the accountability requirements of 10 U.S.C. 2222.

B. Responsible Parties

1. The Head of each DoD Reporting Entity, as defined in subparagraph 030302.A, is responsible for planning, testing, evaluating, remediating, and reporting remediation action progress and results. The entity Head may delegate these responsibilities.
2. The entity Head or delegate may rely on independent internal or external resources (e.g., Service Audit Agency, DoD Inspector General, Independent Public Accounting (IPA) firms) for FFMIA testing and evaluation and should ensure resources employed are objective and sufficiently qualified to perform the evaluation. The Government Accountability Office's (GAO) *Government Auditing Standards* and the American Institute of Certified Public Accountants Statement on Auditing Standards Number 1, Section 210 both provide guidance regarding qualifications for personnel performing program and financial statement audits.

C. Compliance/Remediation Planning and Monitoring

1. The DoD Financial Improvement and Audit Readiness (FIAR) Plan. The FIAR Plan is the Department's comprehensive compliance and remediation plan for:

    a. Improving financial information.

    b. Preparing for future financial statement audits based on incremental efforts focused on end-to-end business process segments, implementing OMB Circular 123, Appendix A (i.e., documenting, testing and strengthening financial controls at the transaction level).

    c. Working concurrently to also achieve FFMIA compliance by end-to-end business process segment.

2. Target Integrated Financial Management System (IFMS). Each DoD Reporting Entity as defined in subparagraph 030302.A, shall document their target IFMS in their FIAR Plan and the DoD Enterprise Transition Plan. The target IFMS is the IFMS the entity plans to be using when the entire Reporting Entity achieves auditability. If a system is not planned to be a component of the target auditable IFMS, then it should not be evaluated based on the following criteria for FFMIA compliance.
    a. Specific system, module, or components of the target IFMS shall be identified and associated with segments and end-to-end business process in the FIAR Plan.
    b. Each system, module, or component of the target IFMS must be recorded in the DoD Financial Management System Inventories maintained in the DITPR in accordance with DoD policies and requirements.
    c. The target IFMS must be consistent with the Financial Management System Inventory reported to OMB annually.

3. Testing Plan. The schedule for testing the individual components or defined group of components of the target IFMS shall be consistent with and in support of the management assertion plans and timelines in the entity's Financial Improvement Plan (FIP) and in the DoD FIAR Plan. Test plans for individual components of the target IFMS must consider the inter-operability of all operational components of the Reporting Entity's target IFMS.

4. Remediation Plan. Testing of individual target IFMS components is expected to identify instances of non-compliance with FFMIA requirements. When such instances are identified, the Reporting Entity shall develop and document corrective actions and include them in their FIP and the DoD FIAR Plan. The remediation plan must specify a completion date for planned compliance with FFMIA requirements in accordance with FIAR Plan milestone guidance.

5. Reporting FFMIA Evaluation Results. Each DoD Reporting Entity must report the results of their evaluation of FFMIA compliance in the Statement of Assurance required by OMB Circular A-123 beginning in fiscal year 2010. If the

agency's systems do not substantially conform to financial systems requirements, the Statement of Assurance must list the reasons for nonconformance and provide the agency's plans for bringing its systems into substantial compliance. Financial management systems include both financial and mixed systems.

D. The FFMIA Compliance Process

1. The OUSD(C), Directorate for Financial Improvement and Audit Reporting (FIAR) shall annually update and publish the Department's FIAR Plan guidance. See FIAR website: http://www.defenselink.mil/comptroller/FIAR/

2. The FIAR Plan guidance shall:

   a. Provide direction for conducting the FIAR Plan Discovery and Correction phase, implementation of OMB Circular A-123, Appendix A, within DoD, and working to achieve FFMIA compliance concurrently with efforts to achieve auditability.
   b. Provide direction for development and preparation of segment management assertion packages and for the conduct of independent segment validations that will eventually be replaced by audits performed in accordance with GAO and OMB guidance.
   c. Contain the following information:
      i. Definition and Documentation. Include requirements for documenting each Reporting Entity target IFMS.
      ii. Evaluation requirements for Reporting Entity target IFMS. In addition to the segments directed for inclusion in the FIAR Plan, each Reporting Entity shall identify other significant segments and the elements of the segments that are significant to their financial management and reporting and include evaluation and corrective action plans in their FIPs. The GAO/President's Council on Integrity and Efficiency (PCIE) Financial Audit Manual, Section 240 provides guidance on how to identify significant elements of the target IFMS.
      iii. Test and Assess Compliance of Material/Significant Segments. The entity Head shall use procedures as described in the FIAR Plan guidance and the GAO/PCIE Financial Audit Manual to assess the compliance of each segment with FFMIA requirements before submitting a Management Assertion that audit readiness was achieved for that segment. See OMB FFMIA Implementation guidance for indicators of FFMIA compliance. (See extract of OMB Circular No. A-127, above.)
      iv. Test and Assess Compliance of Material/Significant Segment Components. Since entire segments may not reach their target state for some time, it may be advantageous for an entity to test and assess individual components of the target segment before the entire target segment is in place. The entity Head shall use guidance and procedures as described in the FIAR Plan and the GAO/PCIE Financial Audit Manual, to assess the compliance of selected process segment components with FFMIA requirements.

v. Reporting Entity Test and Assessment Submissions. Each Reporting Entity should document the procedures used to select the FFMIA requirements applicable to a given segment and exercise care to ensure that there are no gaps of requirements within a segment. At a minimum, entities must test and evaluate the following before submitting a full segment compliance assessment:

(a) Software Acquisitions. Before Acquisition Milestone A, as defined by DoD Instruction 5000.2, "*Operation of the Defense Acquisition System*," software requirements should be evaluated to ensure that they include the FFMIA requirements for the process segments the software will support. Financial Management software acquisitions that have been designated as a Major Automated Information System (MAIS) by the Acquisition Executive must be tested and evaluated for compliance with FFMIA requirements after development and before Acquisition Milestone C.

(b) Processes, Procedures, Controls, and Data Standards. Significant target processes, procedures, controls, and data standards already in existence should be tested and evaluated to ensure they are operating effectively and as designed. This should be scheduled in accordance with the segment plan in the Reporting Entity FIP and FIAR Plan.

(c) Existing Software. Significant existing software components of the target FMS should be evaluated for FFMIA requirement compliance. This should be scheduled in accordance with the segment plan in the Reporting Entity's FIP and FIAR Plan. This applies to both core financial systems and mixed systems.

(d) Third-Party Software Provided as a Service. Entities may rely on FFMIA requirement testing performed by other entities provided that an assessment of the testing scope indicates that all requirements fulfilled by the software for the entity were tested in the previous test. The Reporting Entity remains responsible to ensure that third-party software meets applicable requirements. Upon determining that any third-party software is a significant component of the Reporting Entity's target IFMS, the Reporting Entity shall coordinate with the service provider to conduct appropriate testing of the software.

3. Maintaining Compliance. The FIAR Plan guidance shall prescribe and define mandatory practices for maintaining auditability subsequent to assertion and validation. These same practices shall be applied to maintain compliance with FFMIA requirements.

0304 DEFINITIONS

Integrated Financial Management System (IFMS). The IFMS is a unified set of financial systems and the financial portions of mixed systems encompassing the software, hardware, personnel,

processes (manual and automated), procedures, controls, and data necessary to carry out financial management functions, manage financial operations of the agency and report on the agency's financial status to central agencies, Congress and the public. Unified means that the systems are planned for and managed together, operated in an integrated fashion, and linked together electronically in an efficient and effective manner to provide agency-wide financial system support necessary to carry out the agency's mission and support the agency's financial management needs. The IFMS has the following characteristics:

A. Common Data Elements.
B. Common Transaction Processing.
C. Consistent Internal Controls.
D. Efficient Transaction Entry.

Information Systems is defined as the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Information systems include non-financial, financial, and mixed systems.

Financial Systems:

A. Financial Systems are considered an information system comprised of one or more applications that is used for any of the following:
    1. Collecting, processing, maintaining, transmitting, and reporting data about financial events.
    2. Supporting financial planning or budgeting activities. A
    3. Accumulating, recognizing, and distributing cost management information.
    4. Supporting the preparation of financial statements.
B. Features of a financial system include but are not limited to the following elements
    1. Supports the financial functions required to track financial events, provide financial information significant to the financial management of the agency, and/or required for the preparation of financial statements.
    2. Encompasses automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions.
    3. May include multiple applications that are integrated through a common database or are electronically interfaced, as necessary, to meet defined data and processing requirements.

Non-Financial Systems. An information system that supports non-financial functions of the Federal Government or components thereof and any financial data included in the system are insignificant to agency financial management and/or not required for the preparation of financial statements.

Mixed System. An information system that supports both financial and non-financial functions of the Federal government or components thereof. These are also commonly referred to in DoD as Financial Feeder Systems or Secondary Financial Systems. Financial feeder systems are information systems that support functions with both financial and non-financial aspects, such as

logistics, acquisition, and personnel. They provide key information required in financial processes.

Financial Management System. The financial systems and the financial portions of mixed systems necessary to support financial management.

Federal Accounting Standards. The Federal Accounting Standards are applicable accounting principles, standards, and requirements consistent with US Code Title 31, Subtitle III, Chapter 35, Subchapter II, Section 3511. The Federal Accounting Standard Advisory Board (FASAB) publishes Statements of Federal Financial Accounting Concepts (SFFAC) and Statements of Federal Financial Accounting Standards (SFFAS), as well as Interpretations, Technical Bulletins, and staff guidance.

Financial Event. Any occurrence having financial consequences to the Federal government related to the receipt of appropriations or other financial resources; acquisition of goods or services; payments or collections; recognition of guarantees, benefits to be provided, or other potential liabilities; or other reportable financial activities.

0305 RESPONSIBILITIES

This section provides the responsibilities of the various DoD entities associated with the governance and execution of this policy. As such, the responsibilities are limited to those specific to the governance and execution of this policy, and are not meant to be an exhaustive list of all of the responsibilities of these entities.

Governance: Governance includes the authorities, framework, and processes the DoD employs to monitor, analyze, validate, integrate, and control FFMIA compliance priorities and requirements through the following DoD organizations:

A. OUSD(C) has overall responsibility for the Department's IFMS and provides oversight and direction for the financial improvement and audit readiness initiatives, and is supported by the Business Integration Office (BIO), the FIAR Director, and the Financial Management Investment Review Board (FMIRB).

B. OUSD(C) BIO Directorate supports the OUSD(C) in carrying out its responsibilities for financial improvement, audit readiness and achieving compliance with FFMIA. As the primary oversight body for FFMIA, OUSD(C)/BIO has the following responsibilities:

    1. Issue and update FFMIA compliance policy.
    2. Monitor, analyze, and measure progress of DoD Reporting Entities in achieving compliance with FFMIA.
    3. Report to OMB and Congress, as required by FFMIA

4. Produce, update, and maintain the FIAR Plan to include integrating with the Enterprise Transition Plan (ETP).
5. Ensure DoD Reporting Entity target IFMS FFMIA compliance plans are in alignment with systems and financial statement audit plans and Component FIP, as applicable.
6. Ensure the detailed requirements of the FFMIA are maintained in the Business Enterprise Architecture (BEA).

C. OUSDC, FIAR Directorate is responsible for:

1. Publishing, and updating on an annual basis the FIAR guidance, as required by this policy.
2. Coordinate and integrate testing and remediation plans into the DoD FIAR Plan Tool.
3. Monitor and analyze progress of entity testing and remediation plans.
4. Monitor, analyze, and document entity FFMIA assertions made in accordance with this policy.
5. Define practices for maintaining auditability subsequent to FFMIA assertion and validation.

D. FMIRB is responsible for:

1. Reviewing and monitoring business system and initiative investment programs for compliance with this policy.
2. Approving investments based on compliance with this policy.

Execution. Execution involves the activities, resources, and leadership required to implement the requirements of this policy.

A. DoD Components and Reporting Entities are responsible for developing and executing plans necessary for achieving compliance with FFMIA. These responsibilities include:

1. Develop, maintain, and execute FIPs that also serve as their FFMIA compliance remediation plan in accordance with the FIAR Guidance.
2. Integrate their FIP and FFMIA compliance plans for conducting FFMIA evaluations with the FIAR Plan in accordance with the FIAR Guidance.
3. Develop and maintain the portfolio of financial and mixed systems that comprise the entity's target IFMS.
4. Establish and maintain centralized oversight of the portfolio of systems comprising the entity's target IFMS. This includes development of 5 year plans in accordance with OMB Circular A-130, "Management of Federal Information Resources."
5. Ensure system portfolio and remediation plans are consistent with modernization priorities identified in the DoD ETP.

6. Ensure system portfolio is consistent with the systems reported in the DITPR.
7. Test MAIS financial systems before implementation to ensure that they properly function within the target IFMS, leveraging existing Systems Development Life-Cycle activities where appropriate.
8. Conduct FFMIA certification testing using the GAO/PCIE FAM and FIAR Plan guidance, leveraging existing Systems Development Life-Cycle activities where appropriate.
9. Address FFMIA compliance status and remediation plan in annual Statement of Assurance beginning in fiscal year 2010.
10. Ensure that annual updates to the ETP are in alignment with the FIAR Plan.

B. Defense Finance and Accounting Service (DFAS). The DFAS has the following responsibilities related to FFMIA:

1. Developing and maintaining a DFAS system FFMIA compliance remediation plan that is in synch with Component needs. For each financial and mixed system managed by DFAS, this includes:
   a. Establishment of a Memorandum of Agreement (MOA) with each DoD Reporting Entity supported by each DFAS system.
   b. Conducting compliance testing, as required per MOA, when a system(s) is a significant part of a Reporting Entity's IFMS.
   c. Supporting Reporting Entity end-to-end business process testing (per MOA).

2. Maintaining, in coordination with the OUSD(C) and Business Transformation Agency, the FFMIA requirements in the Business Enterprise Architecture (BEA).

C. Business Transformation Agency (BTA). The BTA has the following responsibilities related to FFMIA:

1. Ensure that annual updates to the DoD ETP are in alignment with the FIAR Plan.
2. Update FFMIA requirements provided by DFAS in the BEA and provide user-friendly access to the requirements to the Reporting Entities.
3. Develop and maintain a BTA Enterprise System FFMIA compliance remediation plan that is in synch with Component needs. For each Enterprise financial and mixed system managed by BTA, this includes:
   a. Establishing an MOA with each DoD Reporting Entity supported by each BTA Enterprise system.
   b. Conducting compliance testing, as required per MOA, when a system(s) is a material part of a Reporting Entity's FMS.
   c. Supporting Reporting Entity end-to-end business process testing (per MOA).

D. DoD Inspector General (DoDIG). The DoDIG is responsible for:

1. Performing system audits (e.g., general and application control and FFMIA) based on Reporting Entity FIPs and the FIAR Plan.

2. Performing FFMIA compliance evaluations as part of financial statement audits and/or oversee evaluations performed by IPAs during financial statement audits. This includes identifying in writing the nature and extent of non-compliance when appropriate.

E. Defense Information Systems Agency (DISA). The DISA is responsible for evaluating FFMIA requirements related to information technology controls and security for significant financial management systems administered by DISA.