

**VOLUME 1, CHAPTER 3: “FEDERAL FINANCIAL MANAGEMENT  
IMPROVEMENT ACT COMPLIANCE”**

**SUMMARY OF MAJOR CHANGES**

Changes are identified in this table and also denoted by [blue](#) font.

Substantive revisions are denoted by an asterisk (\*) symbol preceding the section, paragraph, table, or figure that includes the revision.

Unless otherwise noted, chapters referenced are contained in this volume.

Hyperlinks are denoted by [\*\*\*bold, italic, blue, and underlined font\*\*\*](#).

The previous version dated [October 2020](#) is archived.

<b>PARAGRAPH</b>	<b>EXPLANATION OF CHANGE/REVISION</b>	<b>PURPOSE</b>
All	Streamlined to remove instructional language.	Revision
1.1	Added interdependencies between Federal Financial Management Improvement Act and other compliance requirements.	Addition
2.0	Revised definitions.	Revision
3.3	Revised and streamlined description of Compliance Determination Framework.	Revision
4.0	Streamlined to remove instructional language.	Revision

## Table of Contents

VOLUME 1, CHAPTER 3: “FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT COMPLIANCE” .....		1
1.0	GENERAL.....	3
*1.1	Overview .....	3
1.2	Purpose .....	3
1.3	Authoritative Guidance .....	3
*2.0	DEFINITIONS.....	4
2.1	Financial Management System .....	4
2.2	Core Financial System .....	4
3.0	ACCOUNTING STANDARDS.....	5
3.1	System Transactions.....	5
3.2	FFMIA Compliance .....	5
*3.3	Compliance Determination Framework.....	6
*4.0	RESPONSIBILITIES.....	6
4.1	Office of the Under Secretary of Defense (Comptroller).....	6
4.2	Director of Administration and Management .....	8
4.3	Components.....	8
4.4	Service Organizations .....	9
4.5	Inspector General .....	9
4.6	Hosting Organizations.....	9

## CHAPTER 3

**FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT COMPLIANCE**

## 1.0 GENERAL

## \*1.1 Overview

The Federal Financial Management Improvement Act of 1996 ([FFMIA](#)) is intended to ensure Federal [financial](#) systems provide reliable, consistent and uniform disclosure of financial data using accounting standards. FFMIA requires the Department of Defense (DoD or Department) to implement and maintain [financial](#) systems that comply with Federal Financial Management System Requirements ([FFMSR](#)), applicable Federal accounting standards, and the United States Standard General Ledger (USSGL) at the transaction level. FFMIA requires [DoD management to annually assess and](#) DoD auditors to report on the Department’s compliance as part of financial statement audit reports; and determine, based on the audit report and other information, whether the Department’s financial management systems [substantially](#) comply with FFMIA and, if not, to develop remediation plans as applicable.

While [FFMIA compliance centers on these three standards](#), it is not limited to them. For example, [certain FFMSR are interrelated to and depend on other standards and requirements underpinning the Federal Managers' Financial Integrity Act, the Agency Chief Financial Officers \(CFO\) Act, the Federal Information Security Management Act of 2002 \(FISMA\), and Office of Management and Budget \(OMB\) Circular A-123 requirements.](#)

## 1.2 Purpose

This chapter prescribes the Department’s policy for achieving compliance with FFMIA. It provides the basis for the implementation of FFMIA in order for the Department to generate timely, accurate, and useful [financial](#) information with which the Department leadership can make informed decisions and to ensure accountability on an ongoing basis.

## 1.3 Authoritative Guidance

The requirements prescribed by this chapter are in accordance with the applicable provisions of:

1.3.1. Title 10, United States Code, section 2223(a)(5) ([10 U.S.C. § 2223\(a\)\(5\)](#)) “Information technology: additional responsibilities of Chief Information Officers”

1.3.2. [31 U.S.C § 1115](#) “Federal Government and agency performance plans.”

1.3.3. [31 U.S.C. § 3512](#), “Executive agency accounting and other financial management reports and plans”; with emphasis on sections 801 – 807 (FFMIA).

1.3.4. [31 U.S.C. Chapter 9](#) “Agency Chief Financial Officers.”

1.3.5. [44 U.S.C. Chapter 35, Subchapter III](#) “Confidential Information Protection and Statistical Efficiency.

1.3.6. [44 U.S.C. §3601](#), “Definition.”

1.3.7. [OMB Bulletin No. 22-01](#), “Audit Requirements for Federal Financial Statements.”

1.3.8. [OMB Circular A-123, Appendix D](#), “Management of Financial Management Systems – Risk and Compliance.”

1.3.9. [OMB Circular A-130, Appendix I](#), “Responsibilities for Protecting and Managing Federal Information Resources.

1.3.10. Statement on Standards for Attestation Engagements No. 18, ([SSAE 18, AT-C Section 320](#)) “Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting.”

1.3.11. National Institute of Standards and Technology ([NIST\) Special Publication 800-53](#), Revision 5, “Security and Privacy Controls for Information Systems and Organizations.

1.3.12. U.S. Department of Treasury Financial Manual, Volume 1, Part 6, Chapter 9500 ([1 TFM 6-9500](#)), “Revised Federal Financial Management System Requirements for Fiscal Reporting”

1.3.13. [DoD Instruction \(DoDI\) 8510.01](#),”Risk Management Framework (RMF) for DoD Systems”

## \*2.0 DEFINITIONS

### 2.1 Financial Management System

Financial management systems include the financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, controls, data hardware, software, and support personnel dedicated to the operation and maintenance of system functions. Both financial systems and mixed systems may directly or indirectly trigger a financial event within the system itself or in another system, and may be required to comply with some or all FFMSR.

### 2.2 Core Financial System

Core financial systems and financial systems are synonymous terms and consist of six functional areas: general ledger management, funds management, payment management, receivable management, cost management, and financial reporting. Core financial systems are comprised of one or more software programs (commonly referred to as applications), that are used for:

2.2.1. Collecting, processing, maintaining, transmitting, or reporting data about financial events;

2.2.2. Supporting financial planning or budgeting activities;

2.2.3. Accumulating and reporting costs information; or

2.2.4. Supporting the preparation of financial statements.

### 3.0 ACCOUNTING STANDARDS

#### 3.1 System Transactions

3.1.1. The Department's financial management systems must maintain accounting data at the transaction level. Financial management systems include both financial and mixed systems. All DoD financial events (budgetary and proprietary) must be recorded applying the requirements of the USSGL guidance in the TFM, and DoD USSGL transaction library (See Chapters 4 and 7 for additional guidance).

3.1.2. Every financial relevant business event that results in an automated transaction in a core financial system must general accurate and compliant postings to all relevant budgetary and proprietary general ledger accounts according to the rules defined in the DoD USSGL transaction library guidance.

#### 3.2 FFMIA Compliance

In determining whether the Department's financial management systems substantially comply with FFMIA, management and auditors must consider [the degree to which](#) a system's performance prevents the Department from meeting the specific requirements of FFMIA as listed in paragraph 1.1. [A system may be determined to be substantially compliant with FFMIA when it meets the requirements described in OMB Circular A-123, Appendix D, Attachment 1.](#)

3.2.1. The DoD strategy for FFMIA compliance is integrated with related efforts to achieve auditability and maintain effective Internal Control over Reporting (ICOR) including Internal Control over Financial Reporting (ICOFR). Documentation that supports these related requirements also support FFMIA compliance and may be used to avoid duplication of efforts.

3.2.2. The [DoD ICOFR Guide](#) serves as a standard reference for users involved in financial reporting internal control activities within the DoD. This includes the annual requirements prescribed in the OMB Circular A-123, the FFMIA, and other applicable laws, regulations, and guidance. Its companion, the [DoD Financial Statement Audit Guide](#) is a reference for supporting internal controls based financial statement audits. A system is subject to FFMIA if it is determined to be ICOFR relevant as defined in the DoD ICOFR Guide and performs any business functions aligned to FFMIA compliance requirements, including the FFMSR.

3.2.3. The DoD ICOFR Guide identifies the specific Federal Information System Controls Audit Manual (FISCAM) control activities and techniques needed to address the key ICOR risk areas most likely to impact financial reporting based on the DoD's experience. The remaining FISCAM control activities (identified as "Other Control Techniques for Consideration in a Financial Statement Audit") should be considered by Components when evaluating federal financial systems' compliance with laws and regulations, such as FFMIA and FISMA.

### \*3.3 Compliance Determination Framework

FFMIA Compliance Determination Framework (Framework) assists in providing incremental steps and is designed to walk the user from goal through risk assessment, to conclusion. The risk-based Framework assesses the financial systems integrity risk to comply substantially with FFMIA Section 803(a) requirements. The Framework includes performance results based on annual financial statements, the "Federal Financial Management System Requirements" contained in 1 TFM 6-9500, and other information considered relevant and appropriate. The Framework goals and compliance indicators must to be used during the ongoing operation of the Department's financial management systems. (See OMB Circular A-123, Appendix D, Attachment 1 for additional guidance). The DoD ICOFR Guide defines mandatory practices for maintaining auditability subsequent to assertion and validation. These same practices must be applied to maintain compliance with FFMIA requirements.

### \*4.0 RESPONSIBILITIES

The responsibilities identified in this section are limited to those specific to FFMIA compliance and are not meant to be an exhaustive list of all of the responsibilities of these entities. This includes the authorities and framework that the Department employs to monitor, analyze, validate, integrate, and control FFMIA compliance requirements.

#### 4.1 Office of the Under Secretary of Defense (Comptroller)

4.1.1. The Office of the Under Secretary of Defense (Comptroller) (OUSDC) is supported by the Enterprise Financial Transformation (EFT), the Financial Improvement and Audit Remediation (FIAR) Directorate and the Financial Management Policy and Reporting (FMPR) Directorate. OUSDC is responsible for providing a Department-wide assessment of compliance with the requirements of FFMIA.

4.1.1.1. If the Component financial management systems do not substantially comply with the requirements of Section 803(c), the FFMIA requires that a remediation plan be developed, in consultation with OMB that describes the resources, remedies, and milestones for achieving substantial compliance.

4.1.1.2. OUSD(C) must annually report to OMB the progress made towards resolving identified deficiencies and such progress must be discussed in the Components remediation plan, capital planning and investment control plans, and other planning documents, when applicable. The findings or analysis of noncompliance must be included with a discussion of ongoing remediation activities. Progress towards resolving the deficiencies must not be construed as compliance with FFMIA.

4.1.1.3. Remediation plans are expected to bring the Department's financial management systems into substantial compliance no later than three years after the date a non-compliance determination is made by OUSD(C) or its auditors. However, if OUSD(C), with the concurrence of OMB, determines that the Department's financial management systems cannot be brought into substantial compliance within three years, the Component (in consultation with OUSD(C)) may specify a longer period. In either case, the Component must designate a Component official responsible for bringing the Component's financial management systems into substantial compliance by the date specified and for reporting progress to EFT (acting on behalf of the Defense Business Systems Committee) on a scheduled basis.

#### 4.1.2. EFT:

The Organization of EFT governs the DoD Advancing Analytics (Advana) repository of common enterprise data. See Chapter 10 for additional information about how EFT uses Advana to support FFMIA compliance activities. EFT also acquires, incorporates, and standardizes data to support the business domain areas that align with the organizational structure of the Department. As a result, EFT provides reasonable assurance to consumers that data controls are clearly defined and executed in accordance with FFMIA.

#### 4.1.3. FIAR Directorate

The FIAR Directorate develops, publishes, and issues detailed financial improvement audit strategies, methodologies, and implementation guidance. The FIAR Director, monitors reporting entity FFMIA assertions made and provides internal control training to reporting entities on improving compliance with FFMIA. As a result, the FIAR Directorate, improves the quality of the financial information, with a positive audit opinion as the desired outcome.

#### 4.1.4. FMPR Directorate

The FMPR Directorate develops, publishes, implements, and interprets DoD-wide accounting and finance policies; ensures the DoD Financial Management Regulation (DoD 7000.14-R) is consistent with laws and other applicable guidance. The FMPR Directorate, leads and oversees DoD financial integrity. As a result, FMPR develops, publishes, and interprets DoD-wide financial management improvements and guidance that supports statutory requirements for the Department to audit its full set of financial statements.

## 4.2 Director of Administration and Management

The [Director of Administration and Management \(DA&M\)](#) is the principal management office for the Secretary of Defense responsible for optimizing the business environment across the DoD enterprise. The [DA&M delivers premier program management and oversight, security services, and support functions that enable uninterrupted operations of the Department Headquarters.](#)

## 4.3 Components

4.3.1. Components must establish and maintain financial management systems that substantially comply with FFMIA Section 803(c) requirements. Component systems must be developed to generate reliable, timely and consistent information necessary for the Department to comply with FFMIA requirements. DoD systems must have the ability to prepare [accurate, reliable, and timely](#) financial statements and other required financial and budget reports using information generated by the financial management systems. [Component management must annually test financial management systems for FFMIA compliance as required by OMB Circular A-123, Appendix D.](#)

4.3.2. Components must maintain records of systems and transactional data to comply with FFMIA, financial statement audits, ICOFR, and Internal Control over Financial Systems in:

4.3.2.1. DoD Information Technology Portfolio Repository (DITPR). Components must ensure their [financial](#) system portfolio is [accurately](#) reported in DITPR. DoD financial systems [must review, report, and update appropriately all DITPR FFMIA reporting requirements and DoD business enterprise architecture operational activity assertions that align to federal financial management functions on an annual bases](#) in accordance with 10 U.S.C. § 2223(a)(5).

4.3.2.2. FIAR Systems Database (FSD). Components must utilize FSD to identify, capture, and report on the universe of financially-relevant systems for audits, executive leadership, and Congressional reporting requirements. Owners of each system must maintain the current status of FFMIA compliance in FSD to support annual FFMIA compliance and Department's Annual SOA reporting.

4.3.2.3. Advana. Components must provide [EFT](#) with periodic (minimum quarterly) budgetary and proprietary transactional data for uploading to Advana. See Chapter 10 for additional information.

4.3.3. Components must use 1 TFM 6-9500 in the pre-acquisition, acquisition, and implementation of new financial management solutions (manual or automated). These federal financial management system requirements establish uniform financial systems, standards, and reporting that support the achievement of the DoD financial reporting objectives. In addition, Components must use the Federal Financial Management System Requirements in accordance with OMB Circular A-123.



4.3.3.1. Develop a plan in accordance with OMB Circular A-130, Appendix I.

4.3.3.2. Ensure the system portfolio and remediation plans are consistent with modernization priorities identified in 44 U.S.C. §3601.

4.3.4. Assess internal controls over business processes as well as Information Technology General Controls (ITGC) and IT Application Controls.

4.3.5. Conduct FFMIA certification testing using the Government Accountability Office (GAO) Financial Audit Manual, DoD ICOFR Guide, 1 TFM 6-9500 and DoD Financial Statement Audit Guide, leveraging existing system development life-cycle activities where appropriate.

#### 4.4 Service Organizations

Service Organizations must develop and maintain FFMIA compliance remediation plan in coordination with DoD Components. For each financial system and mixed system managed by Service Organizations a Memorandum of Agreement (MOA) must be established with each DoD Component. As part of the MOA, compliance testing must be conducted to support Component end-to-end business process testing. Service Organizations must provide Components with a Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting and also known as a System and Organizational Controls 1 (SOC 1 Report). The SOC 1 Report evaluates the effect of the controls at the service organization on the user entities' controls for financial reporting.

#### 4.5 Inspector General

The Office of the Inspector General performs FFMIA compliance evaluations as part of financial statement audits and/or oversees evaluations performed by independent public accounting firms during financial statement audits. This includes identifying in writing the nature and extent of non-compliance when appropriate. Inspector General reports to Congress instances and reasons when the Department has not met the intermediate target dates established in the remediation plan required under FFMIA Section 803(c).

#### 4.6 Hosting Organizations

Hosting Organizations provide application hosting services for the DoDs service providers. As a result, hosting organizations are responsible for most of the ITGC over the computing environment in which many financial, personnel, and logistics applications reside. In order for service providers and components to rely on automated controls and documentation within these applications, controls must be appropriately and effectively designed.