Defense Finance and Accounting Service

DFAS 7900.4-M

Financial Management Systems Requirements Manual

Volume 14, Audit Trails and System Controls

August 2015

Strategy, Policy and Requirements ZP

SUBJECT: Description of Requirement Changes

The complete listing and description of the requirements changes, deletions, and additions by chapters and systems requirements can be found below.

All changes in this volume are denoted by bold blue font.

VOLUME 14 - Audit Trails and Systems Controls		
Req Id	**Change Type**	**Reason for Change**
14.01.005	**D - Authoritative Source/Reference Deleted**	
14.01.021	**D - Authoritative Source/Reference Deleted**	
14.01.043	**D - Not Supported by a Correct Source/Reference**	
14.02.091	**D - Authoritative Source/Reference Deleted**	
14.02.100 14.04.014 14.04.024 14.04.027 14.04.031	**D - Not Supported by a Correct Source/Reference**	
14.05.002	**D - Authoritative Source/Reference Deleted**	
14.05.004	**D - Not Supported by a Correct Source/Reference**	
14.05.011 14.05.016	**D - Authoritative Source/Reference Deleted**	
14.05.018	**D - Not Supported by a Correct Source/Reference**	
14.05.021 14.05.035 14.05.039 14.05.043	**D - Authoritative Source/Reference Deleted**	

VOLUME 14 - Audit Trails and Systems Controls		
Req Id	**Change Type**	**Reason for Change**
14.05.046 **14.05.047** **14.05.050** **14.05.052** **14.05.053** **14.05.054** **14.05.055** **14.05.056** **14.05.062** **14.07.004**	**D - Not Supported by a Correct Source/Reference**	
14.07.032	**D - Authoritative Source/Reference Deleted**	

Chart Legend:

A - Added

   These are new requirements due to revised and updated source documents.

C - Changed

   These requirements were contained in previous releases, but were changed for various reasons.

D - Deleted

   These requirements were removed and are no longer required by the source documents.

TABLE OF CONTENTS

AUDIT TRAILS AND SYSTEM CONTROLS INTRODUCTION

Financial management systems must be able to record and keep track of financial transactions and related information to provide a basis for central financial control. Audit trails—documentation of transactions from their inception to final disposition and reporting in the books of original entry are critical to providing support for transactions and account balances.

While audit trails are essential to auditors and system evaluators, they are also necessary for the day-to-day operations of systems. Reliable audit trails permit verification of transactions to ensure that they are properly recorded, classified, coded and posted to all affected accounts. Additionally, audit trails allow for the detection and tracing of rejected or suspended transactions and correction promptly. All transactions, including computer-generated computations, must be traceable to individual source records.

Adequate audit trails allow tracing from source documents of financial events to general ledger account balances through successive levels of summarization and financial reports and statements. Tracing summarized information backward from the reporting entity level to the transaction source level is a tedious and demanding job. However, documentation is accessible through the successive levels of summarization if the audit community has the available resources.

Commensurate with reliable documentation for transactions are adequate systems controls and documentation. Financial management systems must comply with a myriad of functional and technical requirements to ensure that DoD's financial management and accounting objectives are met in an economical and efficient manner. The design of an accounting system must include the required interfaces with other systems or connections within the various segments of the immediate accounting system. System documentation should be detailed and comprehensive and include the internal controls incorporated into the system. Such documentation should be in sufficient detail to be understood by computer programmers and systems accountants assigned to develop applicable software. Documentation also provides information used to test systems to ensure that they process transactions and financial data in accordance with the financial management systems requirements. This volume and other DFAS 7900.4-M volumes financial management systems requirements may be applicable to your system.

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.001		The system must generate an audit trail of transactions recorded as a document moves from its source through all document statuses.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.3.2.1_Verifying Traceability_P	Verify that GL account balances can be traced to aggregated or discrete transactions in agency programmatic systems and that the aggregated or discrete transactions can be traced to the point of entry and source documents consistent with the TFM.	Transaction_Audit_Trails_001
Audit Trails (Transaction Documentation)	14.01.005	D - Authoritative Source/Reference Deleted	DELETED: The system must re-open a closed document to allow further processing against it, without requiring a new or amended document number.	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_004

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.009		To support the Audit Trails process, the system must provide automated functionality to capture all document change events (additions, modifications and cancellations), including the date/time and User ID.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_006

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.014		To support the Document and Transaction Control process, the system must provide automated functionality to suspend documents that fail transaction processing edits, funds control edits, or tolerance checks.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_007

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.021	D - Authoritative Source/Reference Deleted	DELETED: The system must ensure that specific edits are applied by type of transaction in each finance or accounting system. Those transactions failing to pass edits, and/or otherwise not entered, must be controlled and assigned for research and correction and, to the degree feasible, are temporarily, recorded in suspense accounts in the accounting system.	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_009

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.030		To support the Document and Transaction Control process, the system must validate that duplicate documents are not recorded, e.g., by editing document numbers or storing additional information that make the document number unique (as in date stamp on a utility bill).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_015

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.031		To support the Document and Transaction Control process, the system must notify the user when online documents fail funds control edits, transaction processing edits, or tolerance checks. Provide the notification on the document entry screen, and include the nature of each error and the validation level (rejection, warning or information only). Retain errors with the document until they have been resolved.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_016

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.032		To support the Document and Transaction Control process, the system must validate transaction accounting classification elements. Prevent the recording of transactions with missing, invalid or inactive classification elements or values.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_017
Audit Trails (Transaction Documentation)	14.01.034		To support the General Ledger Analysis and Reconciliation process, the system must generate the GL Supporting Documents Report as of the current system date. Parameters include a GL control account and Treasury Account Symbol (TAS) or internal fund code. Result is the GL account balance, and a list of the open documents and balances supporting the GL account balance.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.3.2.2_Verifying Traceability_P	Verify that financial statements and other required financial and budget reports can be traced to GL account balances as required by OMB Circular No. A-123 and as specified in the TFM.	Transaction_Audit_Trails_019

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.039		To support the Document and Transaction Control process, the system must provide automated functionality to define over tolerances for all obligations or by obligation type.	Source: OMBCIRA-123,Att,II; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_024

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.042		The system must provide automated functionality to define tolerances by percentage, dollar amount or quantity for final payments that are less than the referenced obligation document line amounts, and use them to control erroneous de-obligations of the funds.	Source: OMBCIRA-123,Att,I; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_027

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.043	D - Not Supported by a Correct Source/Reference	DELETED: To support the Audit Trails process, the system must provide automated functionality to query document additions, modifications and cancellations. Parameters include: • User ID • Document number • Document type • Change type (add, modify, cancel) • Transaction date range • Accounting period. Results include all parameter values, document numbers, date and time stamps.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_028

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.046		To support the Document and Transaction Control process, the system must provide automated functionality to capture a unique system-generated or agency-assigned document number for each document and document modification.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_031

	AUDIT TRAILS AND SYSTEM CONTROLS REQUIREMENTS						DFAS 7900.4-M, Vol. 14
Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.047		To support the Document and Transaction Control process, the system must provide automated functionality to capture a unique system-generated number to identify each general ledger transaction. Associate one or more general ledger transactions with a document and document modifications.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_032
Audit Trails (Transaction Documentation)	14.01.051		To support the Document and Transaction Control process, the system must provide automated functionality to capture the source system and the source system document number of each interfaced document.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.3.2.1_Verifying Traceability_P	Verify that GL account balances can be traced to aggregated or discrete transactions in agency programmatic systems and that the aggregated or discrete transactions can be traced to the point of entry and source documents consistent with the TFM.	Transaction_Audit_Trails_036

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.052		To support the Document and Transaction Control process, the system must provide automated functionality to capture goods delivery and service performance period start and end dates on documents where the period of performance is a validation for future processing, e.g., • Contracts • Blanket purchase agreements • Reimbursable agreements • Travel orders • Grants.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_037

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.054		To support the Document and Transaction Control process, the system must provide automated functionality to prevent the recording of erroneous transactions by rejecting documents that fail transaction processing edits.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_039

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.055		To support the Document and Transaction Control process, the system must provide automated functionality to allow users to hold documents for completion or processing at a later date. Segregate held from suspended documents.	Source: TFMVol1,Pt2,Ch1500, Sec1520; Source Date: 6/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_040

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.056		To support the Document and Transaction Control process, the system must provide automated functionality to process suspended documents at a later date.	Source: TFMVol1,Pt2,Ch1500, Sec1520; Source Date: 6/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_041

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.057		To support the Document and Transaction Control process, the system must provide automated functionality to allow users to cancel (permanently close) posted documents.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_042

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.058		To support the Document and Transaction Control process, the system must provide automated functionality to allow users to delete held or suspended documents.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_043

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.061		To support the Document and Transaction Control process, the system must provide automated functionality to derive the default accounting period from the transaction date. Prevent user override.	Source: OMBCIRA-123,AppA,II; Source Date: 12/1/2004	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_046

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.062		To support the Document and Transaction Control process, the system must provide automated functionality to record subsequent activity against a document with the transaction date of that activity (e.g., the payment voucher), not the transaction date of the original document (e.g., the referenced obligation).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Transaction_Audit_Trails_047
Audit Trails (Transaction Documentation)	14.01.064		An automated Defense Finance and Accounting Service (DFAS) system must ensure that the preparation of all financial reports is consistent from one reporting period to another reporting period and the same financial information is used as the source for different reports whenever the same information is reported.	Source: DoDFMRVol6A,Ch2, Sub0202; Source Date: 8/1/2011	2.3.2.1_Verifying Traceability_P	Verify that GL account balances can be traced to aggregated or discrete transactions in agency programmatic systems and that the aggregated or discrete transactions can be traced to the point of entry and source documents consistent with the TFM.	Transaction_Audit_Trails_057

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.065		An automated system must ensure that the ending balances for one reporting period will be perpetuated as the beginning balances for the subsequent reporting period and shall be carried forward without change.	Source: DoDFMRVol6A,Ch2, Sub0202; Source Date: 8/1/2011	2.3.2.1_Verifying Traceability_P	Verify that GL account balances can be traced to aggregated or discrete transactions in agency programmatic systems and that the aggregated or discrete transactions can be traced to the point of entry and source documents consistent with the TFM.	Transaction_Audit_Trails_056
Audit Trails (Transaction Documentation)	14.01.066		An automated Defense Finance and Accounting Service (DFAS) system must ensure that all transactions applicable to the effective period of the report have been edited and posted to the official accounting records.	Source: DoDFMRVol6A,Ch2, Sub0202; Source Date: 8/1/2011	1.3.2.3_Making Federal Financial Information Accessible_P	Provide and monitor controls for receiving reviewing requests for, and releasing personally identifiable Federal financial information compliant with the Privacy Act and consistent with OMB Circular No. A-130.	Audit_Trails_System_Controls_049

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.071		To support the Document and Transaction Control process, the system must provide automated functionality to derive the default transaction date from the current system date.	Source: OMBCIRA-123,AppA,II; Source Date: 12/1/2004	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_038

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.072		To support the Document and Transaction Control process, the system must provide automated functionality to capture an agency-specified transaction date.	Source: OMBCIRA-123,AppA,II; Source Date: 12/1/2004	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_009

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.074		To support the Document and Transaction Control process, the system must provide automated functionality to capture the following dates on all transactions: • Transaction date - The date a transaction is effective in the general ledger (i.e., the date a financial event is recognized). • System date - The actual date a transaction is processed by the system. This date is assigned by the computer and may not be modified.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_039

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.075		The system must record transactions in both foreign currency and U.S. dollars in all Core system modules.	Source: TFMVol1,Pt2,Ch3200, Sec3220; Source Date: 6/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_010

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.077		To support the Audit Trails process, the system must provide automated functionality to generate an audit trail of all accounting classification structure additions, changes and deactivations, including the effective dates of the changes.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Maintain_GL_Chart _Of_Accounts_021

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.078		Agency systems must maintain, store, and permit ready retrieval of financial information. The time frames for various parts of this requirement differ depending on the subject matter. The single integrated financial management system must be sufficiently flexible to retain and purge information consistent with varying record keeping requirements.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_048

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.079		The system must produce audit trail reports to support data transferred from external systems to the financial system, including an error listing.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_045

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.083		To support the Treasury Information Maintenance process, the system must provide automated functionality to define transactions that impact the FBWT and are reported on the Bureau of Fiscal Service (Fiscal Service) 224, Partial 224, or through the Government wide Accounting (GWA) system as 'IPAC', 'CA $HLINK II', 'Treasury Disbursing Office (TDO) Payments', or 'Reclassifications'.	Source: TFMVol1,Pt2,Ch5100, Sec5130; Source Date: 6/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Record_Collections_ 009

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.085		To support the Transaction Validation activity, the system must provide the capability to control the correction and reprocessing of all erroneous transactions gathered through interfaces through the use of error/suspense files. Erroneous transactions must be maintained until corrected and posted at the specific request of a user.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_007

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.086		To support the Transaction Validation activity, the system must provide the capability to provide immediate, on-line notification to the user of erroneous transactions obtained through direct data entry. Advise reason for error and provide the ability to enter corrections on-line.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_008

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.087		To support the Transaction Validation activity, the system must provide the capability to provide controls to prevent the creation of initial duplicate transactions. For example, prevent the use of the same unique transaction identification number (e.g., document number).	Source: OMBCIRA-123,Att,II; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_009

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.088		To support the Transaction Validation activity, the system must provide the capability to record the user's identification as part of the transaction record.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_022

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.090		To support the Audit Trail function, the system must provide the capability to identify document input, change and approval by user.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Audit_Trail_002

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.091		To support the System-Generated Transactions process, the system must provide automated functionality to capture start and end dates and posting frequency (monthly, quarterly, or specified number of days) of recurring entries and reversals such as accruals and obligations.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Record_Commitments_Obligations_And_Expenditures_013

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
Audit Trails (Transaction Documentation)	14.01.092		The system must provide the ability, where other methods are unavailable, to retain all records relating to payments to individuals and firms for at least four years and making them available for IRS review.	Source: DoDFMRVol13,Ch7,Sub0705; Source Date: 3/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	NonAppropriated_Funds_001

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.001		To meet Operations requirements, the system must deliver an event logging capability for systems, transactions, tables, and system parameters. The logs must include the following: User ID System date Time Type of activity (i.e., add, modify, delete) Old value New value. (For example, provide a log of all attempts to log onto the system or track changes to the prompt pay interest rate value.)	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_001

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.003		To meet Operations requirements, the system must deliver a process scheduling capability. Allow the agency to define, initiate, monitor and stop system processes (e.g., online availability, batch jobs, and system maintenance).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_003

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.009		To meet Interoperability requirements, the system must process API transactions using the same business rules, program logic, and edits used by the system in processing transactions submitted through the application client.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_004

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.044		Adequate training and appropriate user support must be provided to the users of the 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.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_011

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.051		The system must deliver the capability to process queued jobs (i.e. reports, transaction files from interfacing systems, bulk record updates) with no online performance degradation.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_016

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.059		To meet Documentation requirements, the system must deliver documentation that identifies all software and hardware products needed by an agency to install, operate, access, and maintain the application. Delivered hardware and software documentation must specifically identify those products that are intended to be purchased or licensed as part of the product licensing agreement, and those products needed to meet any technical and functional requirement that must be acquired separately by the agency.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_024

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.060		To meet Documentation requirements, the system must deliver application design documentation. This documentation must include the following: • Description of the application's design/architecture and integrated technologies • Database specifications • Data dictionary • Entity relationship diagrams • Internal file record layouts • Cross references between internal files, database tables and data-entry screens • Program module specifications including firmware and program source code • System flowcharts. Application documentation must identify known problems (software bugs) and recommended work around.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_025

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.061		To meet Documentation requirements, the system must deliver product installation and maintenance documentation. Installation documentation must describe the following items: • Product release content • Third party software configuration requirements • Database installation steps • The directory structure for locating application data, programs, files, tables including drive mappings • Hardware driver installation and configuration • Application security set-up and maintenance • Software configuration instructions • Operating parameter definitions and any other required set-up data • Software build instructions • Vendor supplied configuration tools • Interface processes to be installed • Startup scripts needed to initiate the software • Test steps needed to verify correct installation.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_026

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.062		To meet Documentation requirements, the system must deliver system operations and user manuals. Documentation must explain the following system operations: System start-up Shutdown Monitoring Recovery/re-start Internal processing controls Archiving and application security. User documentation must explain in detail how to execute available functionality in each application component and must cover instructions for the following: Access procedures User screen layout Standard report layout and content Transaction entry Workflow Batch job initiation GL and transaction maintenance Year-end processing Error codes with descriptions Recovery steps Trouble shooting procedures.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_027

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.063		To meet Documentation requirements, the system must deliver documentation updates concurrent with the distribution of new software releases. Release notes must clearly identify all changes made to the system's functionality, operation or required computing hardware and software.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_028

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.067		To meet Infrastructure requirements, the system must ensure the delivered system includes a Structured Query Language (SQL) compliant relational database.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_067

AUDIT TRAILS AND SYSTEM CONTROLS REQUIREMENTS						DFAS 7900.4-M, Vol. 14
Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.068		To adhere to proper Infrastructure functionality, the system must operate in a mainframe environment Operating System (OS).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_068

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.071		To meet Interoperability requirements, the system must deliver a capability to import and process standard transactions generated by other systems.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_063

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.072		To meet Interoperability requirements, the system must deliver data record layouts for all standard transactions that can be accepted by the application's API facility. Transactions must include sufficient data to enable complete validation and processing by the receiving system.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_065

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.074		To meet Interoperability requirements, the system must generate API transaction edit error records using a data layout defined by the vendor (i.e., provide two-way interface support).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_066

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.075		To meet Interoperability requirements, the system must deliver the capability to connect to an agency operated e-mail system. This capability must include the ability to distribute application generated text messages with attached files.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_059

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.077		To adhere to interoperability requirements, the system must deliver an integrated Extensible Markup Language (XML) parsing capability.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_057

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.078		To adhere to interoperability requirements, the system must deliver a capability to exchange data using the Extensible Authentication Protocol.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_056

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.079		To meet operations requirements, the system must maintain internal database consistency at all times. In the event of a system failure the system must have the capability to: • Back out incompletely processed transactions • Restore the system to its last consistent state before the failure occurred • Re-apply all incomplete transactions previously submitted by the user • Validate internal database consistency to ensure duplicate postings are avoided • Report any data or transactions that failed to process completely.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_069

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.080		To meet Operations requirements, the system must Generate online status messages to the operator. Include job or transaction type, name, when processing initiates, when it completes, and any processing errors encountered.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_025

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.082		To meet Operations requirements, the system must deliver common error-handling routines across functional modules. Generate meaningful and traceable error messages that allow the user or \system operator to identify and respond to reported problems.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_071

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.083		To meet operations requirements, the system must deliver a document archiving capability. Include the ability to define, establish, and maintain archival criteria, such as date, accounting period, closed items, and vendors/customers inactive for a specific time period. Archiving of closed or completed detail transactions must not affect related general ledger account balances.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_061

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.084		To meet operations requirements, the system must support data archiving and record retention in accordance with rules published by the National Archives and Records Administration (NARA), GAO, and National Institute of Standards and Technology (NIST).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_062

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.085		To meet operations requirements, the system must deliver the capability to restore archived data based on agency-defined criteria such as date, accounting period, or vendor/customer.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_060

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.086		To meet Operations requirements, the system must maintain and report application usage statistics. Productivity statistics should include concurrent users, job submissions, transactions throughput, and system availability.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_026

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.087		To meet Operations requirements, the system must deliver a capability to override the system date value used to automatically default document effective date and related transaction posting date/period. This capability is intended for system testing.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_072

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.088		The system must deliver the capability to customize system logging features. Allow the agency to specify which parameters (or tables) to log. Allow the agency to turn logging feature on or off as needed.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_058
System Controls and Documentation	14.02.089		The system must provide a capability to replicate all operational data to the continuity of operations program site.	Source: NISTSP800-53,Ch1; Source Date: 4/1/2013	2.3.2.1_Verifying Traceability_P	Verify that GL account balances can be traced to aggregated or discrete transactions in agency programmatic systems and that the aggregated or discrete transactions can be traced to the point of entry and source documents consistent with the TFM.	System_Controls_And_Documentation_074

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.091	D - Authoritative Source/Reference Deleted	DELETED: To support the Internal and External Reporting function, the system must be able to create, compute, and post all necessary financial transactions.	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_And_AR_Reporting_009

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.094		To support the Transaction Validation activity, the system must provide the capability to allow users to define and maintain standard rules that control subsidiary ledger account postings for all accounting events when accounting transactions are recorded in a subsidiary ledger within the system. The process of defining posting rules can be accomplished in a variety of ways, including (but not limited to) using: transaction codes, screen 'templates,' derivation rules, and others.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_003

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.096		To support the Transaction Validation activity, the system must provide the capability to post to the current fiscal year and prior fiscal year concurrently until prior year-end closing is complete while interacting with the system within that fiscal year.	Source: DoDFMRVol1,Ch7,Sub0704; Source Date: 6/1/2009	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_018

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.097		To support the Transaction Validation activity, the system must provide the capability to record different transaction types at the detailed transaction level.	Source: DoDFMRVol1,Ch7,Sub0704; Source Date: 6/1/2009	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_019

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.098		To support the Transaction Validation activity, the system must provide the capability to employ appropriate edits at the point of entry to ensure that all required data have been entered and to validate the accuracy of the data prior to acceptance.	Source: OMBCIRA-123,Att,II; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_021

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.099		To support the Transaction Validation activity, the system must provide the capability to perform validation checks for use of certain general ledger accounts associated with specific authority (e.g., Cashiers fund, borrowing authority) prior to posting a transaction.	Source: OMBCIRA-123,Att,II; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_027

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.100	D - Not Supported by a Correct Source/Reference	DELETED: To support the On-Line Query function, the system must provide the capability to generate reports in accordance with Federal accounting standards and reporting requirements issued by the Director of OMB and/or the Secretary of the Treasury.	Source: DoDFMRVol1,Ch7,Sub0704; Source Date: 6/1/2009	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Online _Query_Capability_0 12

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.101		To support the Security function, the system must provide the capability to permit actions for information system processes, roles, and users associated with the reporting of accounting records to include for example, read, write, append, and delete.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_008

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Controls and Documentation	14.02.102		In accordance with Internal Revenue Service (IRS) Publication 15, (Circular E), Employer's Tax Guide, records of employment taxes must be maintained for a period of 4 years following the due date of such tax or from the date for which such tax has been paid, whichever date is later.	Source: DoDFMRVol13,Ch8,Sub0811; Source Date: 11/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	NonAppropriated_Funds_012
System Controls and Documentation	14.02.103		Documentation on pay must be stored and transferred to the National Personnel Records Center, St. Louis, MO, for 56 years retention in accordance with the National Archives and Records Administration General Records Schedules.	Source: DoDFMRVol13,Ch8,Sub0811; Source Date: 11/1/2013	2.4.1.2_Securing Financial Management System Information_P	Provide and monitor protection of personally identifiable information about individuals collected, maintained, used, and disseminated by the Federal Financial Management System in support of the Privacy Act and consistent with OMB Circular No. A-130.	NonAppropriated_Funds_013

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.016		An automated accounting must incorporate records management and archival functions into the design, development, and implementation of the information systems.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_007

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.019		An automated accounting system must ensure that records management programs provide adequate and proper documentation of agency financial activities.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_010
General Controls	14.03.020		An automated accounting system must limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.2_Securing Financial Management System Information_P	Provide and monitor protection of personally identifiable information about individuals collected, maintained, used, and disseminated by the Federal Financial Management System in support of the Privacy Act and consistent with OMB Circular No. A-130.	General_System_Controls_011

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.022		Agencies will limit collection of information, which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.2_Securing Financial Management System Information_P	Provide and monitor protection of personally identifiable information about individuals collected, maintained, used, and disseminated by the Federal Financial Management System in support of the Privacy Act and consistent with OMB Circular No. A-130.	General_System_Controls_013
General Controls	14.03.026		All components of an agency's integrated financial management system must provide complete, accurate, and prompt generation and maintenance of acquisition/financial records and transactions.	Source: NISTSP800-53,AppI; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_030

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.029		All components of an agency's integrated financial management system must provide Adequate management controls, including internal and security controls, policies, and procedures intended to protect the agency's key systems, data, and interfaces from disruption and unauthorized access or alteration, as prescribed in a variety of statutes and regulations, including, but not limited to, OMB Circulars A-123 and A-130.	Source: NISTSP800-53,Ch1; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_024

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.034		With regard to security and internal controls, the system must provide flexible security facilities to control user access at varying degrees including: overall system access, capability to perform specific functions (inquiry, update), and access to certain functionality related to acquisitions and finance.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Record_Budget_Authority_And_Allocate_Funds_044

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.035		With regard to security and internal controls, the system must provide capability to define access to specific functions by user name, class of user, and position related to funds control and budgetary accounting.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013Source: 48CFRVol1,Ch1,Pt7,Subpt7.4; Source Date: 8/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Record_Budget_Authority_And_Allocate_Funds_045

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.036		With regard to security and internal controls, the system must provide for multiple levels of approvals based on user-defined criteria, including dollar limits, type of document processed, etc.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Record_Budget_Authority_And_Allocate_Funds_046

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.037		With regard to security and internal controls, the system must provide the capability to perform: reconciliation routines for internal participant accounts, ledgers, and funds; and to identify unsuccessful reconciliations via error log or error report.	Source: OMBCIRA-123,Att,II; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Record_Budget_Authority_And_Allocate_Funds_047

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.038		With regard to security and internal controls, the system must establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against anticipated threats or hazards to record security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained	Source: NISTSP800-53,AppG; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Record_Budget_Authority_And_Allocate_Funds_048

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.039		With regard to security and internal controls, the acquisition/financial must provide a mechanism to monitor changes to software coding and the responsible individual (authorized user).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_029

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.044		To support the Document Referencing and Modification process, the system must provide automated functionality to alert the user concerning certain processing failures.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_012

			AUDIT TRAILS AND SYSTEM CONTROLS REQUIREMENTS			DFAS 7900.4-M, Vol. 14	
Chapter	**Req Id**	**Change Type**	**Requirement**	**Sources**	**Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)**	**Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)**	**DFMIG Rule Name**
General Controls	14.03.049		To meet User Interfaces requirements, the system must comply with Section 508 of the Rehabilitation Act, as detailed in 36 CFR 1194, Subpart B.	Source: 36CFRVol3,ChXI,Pt1 194; Source Date: 8/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_020

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.057		To meet Workflow/Messaging requirements, the system must deliver the capability to define multiple approval levels to a single user. Prevent a user from applying more than one level of approval to the same document in order to conform to the principle of separation of duties. For example, a disbursing officer must not be allowed to certify payment of an invoice he/she entered, and a certifying officer must not be allowed to schedule a payment he/she certified.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_017

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.058		To meet Workflow/Messaging requirements, the system must deliver a workflow calendaring capability to generate date-based process exception reports and alerts. For example, notify an accounts payable office when invoices are held over 30 days with no matching receiving report.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_018

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.060		To meet Workflow/Messaging requirements, the system must deliver the capability to route action requests/status messages internally to individuals, groups or external trading partners. Supported communications channels must include agency e-mail, Blackberry, internal application messaging.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_023

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.061		To meet Workflow/Messaging requirements, the system must deliver the capability to generate workflow event-based user alerts. For example, at the point an emergency travel voucher is approved, electronically notify the affected traveler.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_022

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.062		To meet Workflow/Messaging requirements, the system must deliver the capability to generate user alerts based on agency defined thresholds (i.e., trigger events). For example, electronically warn a budget officer when available funds reach 50% of the allotment.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_021

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.064		To adhere to the proper Workflow/Messaging functionality, the system must generate auditable records of changes made to the workflow approval routing design.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_019

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.065		To adhere to the proper Workflow/Messaging functionality, the system must ensure the delivered system complies with the current Workflow Management Coalition (WFMC) Workflow Standard - Interoperability.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	General_System_Controls_018

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.066		To meet Document Management requirements, the system must deliver the capability to index and store file reference materials received or generated by the agency in electronic format.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_021

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.067		To adhere to the proper Document Management functionality, the system must deliver the capability to electronically image, index and store file reference materials delivered in a hard copy format (e.g., a signed contract, bill of lading, vendor invoices).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_022

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.068		To adhere to the proper Document Management functionality, the system must deliver the capability to notify the user of the presence of associated document images. Deliver on-screen display of imaged material.	Source: 36CFRVol3,ChXI,Pt1194; Source Date: 8/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Controls_And_Documentation_023

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.072		To support the System-Generated Transactions process, the system must provide automated functionality to generate recurring entries and reversals in future accounting periods (e.g., payroll and travel accruals), when the specified transaction dates are reached. This is to include entries that cross fiscal years.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Record_GL_Journal _Entries_003

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.073		To support the Transaction Validation activity, the system must provide the capability to reject a transaction or provide a warning message when attempting to post a transaction that would cause general ledger debits and credits to be out-of-balance at a level below the TAS/TAFS (e.g., organization level).	Source: NISTSP800-53,Ch2; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_024

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.074		To support the Records Retention function, the system must provide temporary restoration to the on-line system for browsing and reporting.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Records_Retention_001

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.075		To support the Records Retention function, the system must provide retention of system records in accordance with Federal regulations established by National Archives and Records Administration (NARA), Government Accountability Office (GAO) and others. Prevent the purging of transactions prior to the proper period in accordance with regulations governing the retention of documents and transactions.	Source: DoDFMRVol1,Ch9,Sub0902; Source Date: 8/1/2011Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Records_Retention_002

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.076		To support the Security function, the system must provide the capability to prevent the alteration of financial data (i.e., voids) except through the posting of transactions that are entered through the normal edit and update process under proper security.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_011

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
General Controls	14.03.077		To support Security function, the system must provide the capability to provide confidential Internet based communication from customer to system.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_016

	AUDIT TRAILS AND SYSTEM CONTROLS REQUIREMENTS					DFAS 7900.4-M, Vol. 14	
Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.013		The system must deliver the capability to receive vendor invoices and payments from the public via the Internet.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Access_011

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.014	D - Not Supported by a Correct Source/Reference	DELETED: The system must support secure Internet access to the integrated ad hoc data query facility.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System_Controls_019

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.015		The system must support operations via a Virtual Private Network (VPN) system capability for secure remote access.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_020

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.016		The system must deliver the capability to use Public Key Infrastructure technology to control system access.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_021

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.024	D - Not Supported by a Correct Source/Reference	DELETED: To meet Ad Hoc Query requirements, the system must deliver the capability to download selected query data. Reformat downloaded query information for direct access by common desktop applications (e.g., spreadsheet, ASCII text, ',' delimited).	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_027

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.027	D - Not Supported by a Correct Source/Reference	DELETED: To meet Ad Hoc Query requirements, the system must deliver the following ad hoc query interface features: • Graphical display of data sources • The ability to 'point and click' on selectable table, data, and link objects for inclusion in a custom query, and • An active data dictionary to provide users with object definitions.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_028

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.031	D - Not Supported by a Correct Source/Reference	DELETED: To effectively support Ad-Hoc Query Capability, the system must support the use of electronic media and formats, including public networks, as appropriate, in order to make government information more easily accessible and useful to the public.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Adhoc_Query_Capability_007

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.032		To support the Security function, the system must provide the capability to allow entry into system only to those individuals who are authorized and only during times authorized.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_001

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.033		To support the Security function, the system must provide the capability to perform annual revalidation of the user.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_002

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.034		To support the Security function, the system must provide the capability to maintain a history of password changes over a specified amount of time and preclude the consecutive use of the same password, including changes and lost passwords.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_003

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.035		To support the Security function, the system must provide the capability to require the use of unique user identifications and passwords for authentication purposes. Passwords must be non-printing and non-displaying. The application must allow for the enforcement of password standards (e.g., minimum length and use of alpha, numeric and special characters). The application must also allow for the establishment of a specified period for password expiration to provide changes on a regular basis, accommodate prohibiting the user from reusing recent passwords and be capable of periodic change, at option of user, and of mandatory change, at the option of the system administrator after a specified period of time.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_004

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Access	14.04.037		To support the Security function, the system must provide the capability to alert and record when invalid access is attempted or when user ID limit is exceeded.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_010

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.001		To meet General Design/Architecture requirements, the Core system must ensure the delivered system is modular, highly scalable and incorporates an open-systems architecture.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System_Controls_040

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.002	D - Authoritative Source/Reference Deleted	DELETED: To meet General Design/Architecture requirements, the Core system must ensure the delivered system is customizable to meet agency-defined business practices. Agency customizable features must be table/parameter driven.	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_041

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.003		To meet General Design/Architecture requirements, the Core system must ensure the delivered system is upgradeable to accommodate changes in laws, regulations, best practices or new technology.	Source: OMBCIRA-123,Att,II; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Design_and _Architecture_002

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.004	D - Not Supported by a Correct Source/Reference	DELETED: To meet General Design/Architecture requirements, the Core system must ensure the delivered system generates output reports, query results and data files using multiple formats as specified by functional requirements. Specified formats can include online display, printed report, Portable Document Format (PDF), MS Word, Excel, ASCII or delimited text file. In cases where an output format is not specified within a requirement, the requested information must be viewable to the agency online, using the application user interface.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_042

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.005		To meet General Design/Architecture requirements, the Core system must deliver fault-free performance in the processing of date and date related data (including, calculating, comparing, and sequencing) by all hardware and software products included as part of the application both individually and in combination (i.e., be Y2K compliant).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System_Controls_043

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.007		The system must deliver a reports management capability to enable online retrieval, viewing, re-printing, and permanent archiving of system-generated reports.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_046

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.009		The system must have the capability to identify and handle error conditions in an expeditious manner through the use of error messages and error logs without providing information that could be exploited by adversaries.	Source: NISTSP800-53,AppE; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_050

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.011	D - Authoritative Source/Reference Deleted	DELETED: The system must provide the capability for a user with special authorization to establish and maintain an accounting classification structure that includes the elements described in the Common Government-wide Accounting Classification (CGAC) structure document.	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_033
System Design and Architecture	14.05.013		The system must provide automated functionality that controls the use of accounting classification elements based on the guidance provided by the U.S. Government Standard General Ledger (USSGL). Each recorded transaction must be generated with the appropriate accounting classification elements according to the rules defined in the USSGL guidance.	Source: DoDFMRVol1,Ch7,Su b0704; Source Date: 6/1/2009	1.1.2.2_Posting GL Transactions_P	Post GL proprietary, budgetary, and memorandum account transactions consistent with USSGL account attributes, account transaction codes, account transaction categories, and account transaction subcategories as defined in the TFM.	Audit_Trails_System _Controls_035

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.015		The system must provide the capability to maintain the common government-wide and agency-specific data relationships prescribed in the Common Government-wide Accounting Classification (CGAC) document guidance, including the following:: -Treasury Account Symbol (TAS) to multiple internal funds - Internal fund to multiple USSGL attributes and fund attributes -Program to multiple USSGL attributes, internal funds, projects, organizations, or activities -Strategic goal to multiple programs and projects. (Removed data elements from requirement. List of specific data elements will be included in the functional specification document.)	Source: TFMVol1,Pt2,Ch1500, Sec1515; Source Date: 6/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_007

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.016	D - Authoritative Source/Reference Deleted	DELETED: The system must provide the capability for a user with special authorization to establish and maintain standard (OMB Circular No. A-11) object class codes and (agency-specific) object class extension codes consistent with the Common Government-wide Accounting Classification (CGAC) structure document.	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System_Controls_037

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.018	D - Not Supported by a Correct Source/Reference	DELETED: The financial system must provide automated functionality to query documents to allow for the assurance that transactions are processed accurately and that the data is valid and complete.	Source: OMBCIRA-123,Att,II; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Perform_Periodic_GL_Postings_012

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.019		To support the System-Generated Transactions process, the system must provide automated functionality to reverse transactions and alert the user when a modification has occurred.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Perform_Periodic_GL_Postings_018
System Design and Architecture	14.05.020		To support the Treasury Information Maintenance process, the system must provide automated functionality to maintain data in accordance with standards used by the agency.	Source: TFMVol1,Pt2,Ch1500, Sec1515; Source Date: 6/1/2015	1.1.2.2_Posting GL Transactions_P	Post GL proprietary, budgetary, and memorandum account transactions consistent with USSGL account attributes, account transaction codes, account transaction categories, and account transaction subcategories as defined in the TFM.	Perform_Periodic_GL_Postings_036

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.021	D - Authoritative Source/Reference Deleted	DELETED: To support the System-Generated Transactions process, the system must provide automated functionality to deliver the capability to send/receive financial transactions from Government wide mandated applications: • Central Contractor Registration (CCR) • Electronic Certification System (ECS) • Federal Agencies Centralized Trial Balance System I (FACTS I) • Federal Agencies Centralized Trial Balance System II (FACTS II) • Government Online Accounting Link System (GOALS II) • Intra-governmental Payment and Collection System (IPAC) • Treasury Offset Program (TOP) • Secure Payment System (SPS).	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Perform_Periodic_GL_Postings_043

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.025		To support the Internal and External Reporting function, the system must have the capability to control the flow of information within the system and and between interconnected systems in accordance with applicable policy.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_And_AR_Reporting_007
System Design and Architecture	14.05.026		To support the Internal and External Reporting function, the system must be able to support provision of data for the preparation of consolidated financial statements as required by the Federal Accounting Standards Advisory Board (FASAB) and the current Office of Management and Budget (OMB) Bulletin on Form and Content of Agency Financial Statements requirements.	Source: DoDFMRVol1,Ch7,Sub0706; Source Date: 6/1/2009	1.1.2.2_Posting GL Transactions_P	Post GL proprietary, budgetary, and memorandum account transactions consistent with USSGL account attributes, account transaction codes, account transaction categories, and account transaction subcategories as defined in the TFM.	Revenue_And_AR_Reporting_011

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.030		To support the Internal and External Reporting function, the system must provide reliable and timely financial information and consistently make the data available for decision making.	Source: DoDFMRVol1,Ch7,Sub0704; Source Date: 6/1/2009	1.3.2.1_Making Federal Financial Information Accessible_P	By implementing technical standards and requirements specified in the Code of Federal Regulations (CFR), provide access to Federal financial information to Federal employees and members of the public with disabilities comparable to that provided to Federal employees and members of the public who are not individuals with disabilities.	Revenue_And_AR_ Reporting_021
System Design and Architecture	14.05.032		To support the Internal and External Reporting function, the system must provide the capability to report process compatibility with both database and application security protocols.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_And_AR_ Reporting_023

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.033		To support the Internal and External Reporting function, the system must provide the capability to perform exception and data ranking reporting based on user-defined parameters.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_And_AR_Reporting_024

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.034		To support the Internal and External Reporting function, the system must provide the capability to define and modify customized reports.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_And_AR_Reporting_025
System Design and Architecture	14.05.035	D - Authoritative Source/Reference Deleted	DELETED: To support the Deposit Account Function, the system must provide the capability to provide monthly statements of transaction activity in paper and/or electronic form.	Source: ; Source Date:	2.2.4.1_Establishing Receivables_DI	Capture Federal Government receivable information (for example, receivable type and customer information) to support agency management of and reporting on receivables to Treasury consistent with the TFM and as required by OMB Circular No.A-129 and the CFR.	Deposit_Account_Function_005

	AUDIT TRAILS AND SYSTEM CONTROLS REQUIREMENTS					DFAS 7900.4-M, Vol. 14	
Chapter	**Req Id**	**Change Type**	**Requirement**	**Sources**	**Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)**	**Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)**	**DFMIG Rule Name**
System Design and Architecture	14.05.036		To support the Transaction Validation activity, the system must provide the capability to interface with the system to record transactions consistent with USSGL posting rules.	Source: DoDFMRVol1,Ch7,Sub0704; Source Date: 6/1/2009	1.1.2.2_Posting GL Transactions_P	Post GL proprietary, budgetary, and memorandum account transactions consistent with USSGL account attributes, account transaction codes, account transaction categories, and account transaction subcategories as defined in the TFM.	Revenue_AR_Transaction_Validation_002
System Design and Architecture	14.05.037		To support the Transaction Validation activity, the system must provide the capability to allow users to define and process system-generated transactions, such as automated accruals (e.g., interest accrual entries), pre-closing and closing entries, and transactions that generate other transactions in those cases where a single transaction is not sufficient.	Source: DoDFMRVol1,Ch7,Sub0704; Source Date: 6/1/2009	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_005

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.038		To support the Transaction Validation activity, the system must provide the capability to validate the fields for all accounting classification elements required to process the transaction prior to posting (e.g., fields pertaining to Treasury Account Symbol/Treasury Appropriation Fund Symbol (TAS/TAFS), revenue source, invoice number, debtor or customer code and organization).	Source: OMBCIRA-123,Att,II; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_011

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.039	D - Authoritative Source/Reference Deleted	DELETED: To support the Transaction Validation activity, the system must provide the capability to enter, edit, and store transactions in the current accounting period for automatic processing in a future accounting period for one-time events and/or monthly recurring entries.	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_012

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.040		To support the Transaction Validation activity, the system must provide the capability to capture transaction dates (effective date of the transaction) and posting dates (date transaction forwarded to the system or posted to the general ledger).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_014

	AUDIT TRAILS AND SYSTEM CONTROLS REQUIREMENTS					DFAS 7900.4-M, Vol. 14	
Chapter	**Req Id**	**Change Type**	**Requirement**	**Sources**	**Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)**	**Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)**	**DFMIG Rule Name**
System Design and Architecture	14.05.041		To support the Transaction Validation activity, the system must provide the capability to determine (automatically) the posting date from the system date for all transactions. Automatically associate a default accounting period for each transaction, but allow authorized user to override.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_015

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.042		To support the Transaction Validation activity, the system must provide the capability to backup and restore data entries input into the system.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_016

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.043	D - Authoritative Source/Reference Deleted	DELETED: To support the Transaction Validation activity, the system must provide the capability to permit posting to the current and prior months concurrently until the prior month closing is complete while interacting with the system within that fiscal year.	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_017

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.044		To support the transaction validation activity utilizing effective intenral controls, the system must reliably process and track transactions in compliance with applicable laws and regulations.	Source: OMBCIRA-123,Att,II; Source Date: 5/1/2008	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Transaction_Validation_025

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.046	D - Not Supported by a Correct Source/Reference	DELETED: To support On-Line Query Capability, the system must provide the capability to record all transactions for a specific accounting record.	Source: DoDFMRVol1,Ch7,Sub0705; Source Date: 6/1/2009	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Online _Query_Capability_0 01

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.047	D - Not Supported by a Correct Source/Reference	DELETED: To support On-Line Query Capability, the system must provide the capability to assign user level capability for ad hoc query access.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Online _Query_Capability_0 04

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.050	D - Not Supported by a Correct Source/Reference	DELETED: To effectively support Ad-Hoc Query Capability, the system must provide data origin and integrity by returning information in response to name and address resolution queries.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Adhoc _Query_Capability_0 02

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.052	D - Not Supported by a Correct Source/Reference	DELETED: To effectively support Ad-Hoc Query Capability, the system must support graphical output display on the desktop. Output display should also support dynamic report reformatting, regrouping and drill-down to detail records from summary report lines.	Source: 36CFRVol3,ChXI,Pt1194; Source Date: 8/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Adhoc_Query_Capability_004

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.053	D - Not Supported by a Correct Source/Reference	DELETED: To effectively support Ad-Hoc Query Capability, the system must allow authorized users to download selected financial data. This download capability must be able to automatically reformat downloaded information for direct access by common desktop applications (e.g., American Standard Code for Information Interchange (ASCII) formatted).	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Adhoc _Query_Capability_0 05

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.054	D - Not Supported by a Correct Source/Reference	DELETED: To effectively support Ad-Hoc Query Capability, the system must provide the ability to preview a report, form, or other query result before printing.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Adhoc _Query_Capability_0 06

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.055	D - Not Supported by a Correct Source/Reference	DELETED: To provide additional Ad-Hoc Query Capability, the system must provide the capability to allow users to automatically distribute copies of report/query results via e-mail to multiple pre-identified individuals or groups.	Source: OMBCIRA-130,8; Source Date: 11/1/2000	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Adhoc_Query_Capability_008

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.056	D - Not Supported by a Correct Source/Reference	DELETED: The system must provide the ability to "point and click" on selectable tables, data, and link objects for inclusion in a custom query.	Source: 36CFRVol3,ChXI,Pt1 194; Source Date: 8/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Design_and _Architecture_001

	AUDIT TRAILS AND SYSTEM CONTROLS REQUIREMENTS					DFAS 7900.4-M, Vol. 14	
Chapter	**Req Id**	**Change Type**	**Requirement**	**Sources**	**Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)**	**Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)**	**DFMIG Rule Name**
System Design and Architecture	14.05.057		To support Interface requirements, the system must provide the capability to provide for uploading and downloading data to other systems and databases in a personal computer environment.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Interface_Requirements_003

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.058		To support Interface requirements, the system must provide the capability to provide controls over interfaced data to ensure that files are transmitted by an authorized source to an authorized destination and they are complete and not duplicates. In addition, controls over each file should ensure (1) the number of transactions in the file matches control records; (2) the dollar total of transactions in the file matches control records; (3) the sender is notified of any erroneous transactions; and (4) erroneous transactions are automatically returned to the sender.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Interface_Requirements_005

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.059		To support Interface requirements, the system must provide the capability to provide an application user interface that complies with the software application standards required by section 508 of the Rehabilitation Act, as detailed in 36 CFR 1194, subpart A.	Source: 36CFRVol3,ChXI,Pt1 194; Source Date: 8/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Interfa ce_Requirements_00 6

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.060		To support Interface requirements, the system must provide the capability to interface with other existing on-line databases that validate sources of data on vendors doing business for the government, for the exchange of identification data and EFT routing information in business transactions and other data elements required by OMB's 'Business Rules for Intragovernmental Transactions.'	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Interface_Requirements_007

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.061		To support Interface requirements, the system must provide the capability to link to other applications and data sources (e.g., strategic plans, performance measures and data warehouse).	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Interface_Requirements_008

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.062	D - Not Supported by a Correct Source/Reference	DELETED: To support the Security function, the system must provide the capability to query the audit log by type of access, date and time stamp range, user identification, or terminal ID.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_014

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Design and Architecture	14.05.063		To support the Security function, the system must provide the capability to comply with Federal Financial Management Improvement Act(FFMIA) standards and the standards promulgated by the Federal Accounting Standards Advisory Board (FASAB).	Source: OMBCIRA-123,Att,III; Source Date: 12/1/2004	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_015

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Performance	14.06.001		To meet the System Performance requirements, the system must process the agency's specified accounting workload without adversely impacting projected online response time.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_029

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Performance	14.06.002		To meet the System Performance requirements, the system must process all scheduled work (e.g., batch jobs) within an agency specified processing window. Scheduled work can include: • Daily systems assurance reports • Daily backups • Daily interface processing • Core GL posting • Table updates • Standard reporting.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_030

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Performance	14.06.003		To meet the System Performance requirements, the system must maintain the agency's specified current and historical financial data (e.g. general ledger records, documents, transactions, lines, and vendor records) storage needs with no degradation to online or batch processing performance.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_031

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Performance	14.06.004		To meet the System Performance requirements, the system must support concurrent access to functional modules for the agency's specified user community.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_032

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Performance	14.06.005		The system must deliver computing performance metrics for platforms and systems environments that the application is certified to run on. Performance metrics provided by the vendor should describe: Transaction processing throughput capacity, Expected workstation client response time by transaction type, Data storage capacity, and Limitations on concurrent user connectivity.	Source: NISTSP800-53,AppG; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Performance _001

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.001		To meet security requirements, the Core system must deliver integrated security functionality compliant with the National Institute of Standards and Technology (NIST) Security Standards. Note: The DoD the security controls published in DoDI 8500.2, "Information Assurance (IA) Implementation," for all DoD information systems based on information sensitivity/classification and the impact or effect on mission success, which is consistent with NIST security standards as confirmed by letter dated June 6, 2007 from NIST to DoD CIO.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_047

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.002		To meet Security requirements, the Core system must ensure that the management, operations and technical baseline security controls are implemented in accordance with Federal Information Processing Standards (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems and other current NIST guidance on selecting the appropriate security controls.	Source: NISTSP800-53,AppI; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Security_005

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.003		To meet security requirements, the Core system must deliver the capability to control function access (e.g., system modules, transactions, approval authorities) and data access (i.e., create, read, update, delete) by assigned: • User ID • Functional role (e.g., payable technician) or • Organization. Enable the agency to define access rules based on any combination of these attributes.	Source: NISTSP800-53,AppI; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_022

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.004	D - Not Supported by a Correct Source/Reference	DELETED: To meet security requirements, the Core system must ensure that the appropriate security controls are consistently enforced in all modules, including software used for ad-hoc data query/report generators.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_023

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.005		To meet Security requirements, the Core system must deliver the capability to restrict access to sensitive data elements, such as social security numbers, banking information by user ID, assigned role or organization.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Audit_Trails_System _Controls_024

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.008		To meet security requirements, an automated system must incorporate technical, operational, and management controls into the application and application rules (as appropriate) to prevent harm from authorized individuals engaged in improper activities, whether intentional or accidental. Examples of such controls are: • separation of duties, • least privilege and • individual accountability.	Source: OMBCIRA-130,AppIII; Source Date: 8/1/2015	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Security_007
System Security	14.07.011		To meet security requirements, an automated system must provide adequate security to protect government information, commensurate with the risk and magnitude of harm, which could result from the loss, misuse, unauthorized access to, or modification of such information.	Source: OMBCIRA-130,8; Source Date: 11/1/2000Source: OMBCIRA-130,AppIII; Source Date: 8/1/2015	1.3.2.3_Making Federal Financial Information Accessible_P	Provide and monitor controls for receiving reviewing requests for, and releasing personally identifiable Federal financial information compliant with the Privacy Act and consistent with OMB Circular No. A-130.	System_Security_004

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.012		To meet system security requirements, all agencies must implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored or disseminated in general support systems and major applications. Each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management (OPM). Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives. Note: The DoD implements this OMB requirement through the DoD IA Program.	Source: OMBCIRA-130,AppIII; Source Date: 8/1/2015	1.3.2.3_Making Federal Financial Information Accessible_P	Provide and monitor controls for receiving reviewing requests for, and releasing personally identifiable Federal financial information compliant with the Privacy Act and consistent with OMB Circular No. A-130.	System_Security_006
System Security	14.07.015		All Agencies must implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored or disseminated.	Source: OMBCIRA-130,AppIII; Source Date: 8/1/2015	1.3.2.3_Making Federal Financial Information Accessible_P	Provide and monitor controls for receiving reviewing requests for, and releasing personally identifiable Federal financial information compliant with the Privacy Act and consistent with OMB Circular No. A-130.	General_System_Controls_002

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.019		The use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication must be in accordance with published DoD policy and procedures. These technologies must be incorporated in all new acquisitions and upgrades whenever possible.	Source: DoDD8500.01E; Source Date: 10/1/2002	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Security_009

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.020		To meet system security requirements, foreign exchange personnel and representatives of foreign nations, coalitions or international organizations may be authorized access to DoD information systems containing classified or sensitive information only if all of the following conditions are met: • Access is authorized only by the DoD Component Head in accordance with the Department of Defense, the Department of State (DoS), and Director of Central Intelligence (DCI) disclosure and interconnection policies, as applicable. • Mechanisms are in place to strictly limit access to information that has been cleared for release to the represented foreign nation, coalition or international organization, (e.g., North Atlantic Treaty Organization) in accordance with DoD Directive 5230.11, for classified information, and other policy guidance for unclassified information such as reference DoD Directive 5230.20E and DoD Instruction 5230.27.	Source: DoDD8500.01E; Source Date: 10/1/2002	1.3.2.3_Making Federal Financial Information Accessible_P	Provide and monitor controls for receiving reviewing requests for, and releasing personally identifiable Federal financial information compliant with the Privacy Act and consistent with OMB Circular No. A-130.	System_Security_010

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.025		All Information Assurance (IA) or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11. Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; Purchase contracts must specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership (NIAP) Assurance Maintenance Program. IA must be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated GOTS or COTS IA and IA-enabled IT products. These products should provide for the availability of the systems, ensure the integrity and confidentiality of information, and ensure the authentication and non-repudiation of parties in electronic transactions.	Source: DoDD8500.01E; Source Date: 10/1/2002Source: NSTISSP11; Source Date: 7/1/2003	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Access_010

AUDIT TRAILS AND SYSTEM CONTROLS REQUIREMENTS						DFAS 7900.4-M, Vol. 14	
Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.026		All DoD information systems must be implemented using the baseline DoD Implementing Agency controls in accordance with DoDI 8500.2.	Source: DoDI8500.2,5; Source Date: 2/1/2003Source: DoDI8510.01,4; Source Date: 11/1/2007	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Security_001

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.027		All DoD information systems must be certified and accredited in accordance with DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP).	Source: DoDD8500.01E; Source Date: 10/1/2002	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Security_012

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.028		All DoD ISs with an authorization to operate (ATO) must be reviewed annually to confirm that the IA posture of the IS remains acceptable. Reviews will include validation of IA controls and be documented in writing.	Source: DoDI8510.01,4; Source Date: 11/1/2007	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Security_002

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.029		The head of each [Federal] agency must develop and maintain an inventory of major information systems. Note: for major DoD IS, the system is considered to be compliant with this requirement if it is registered in the DoD Information Technology Portfolio Registry (DITPR).	Source: PL107-347,Sec305; Source Date: 12/1/2002	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	System_Security_003

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.032	D - Authoritative Source/Reference Deleted	DELETED: To support the Security function, the system must provide the capability to comply with the National Institute of Standards and Technology (NIST) Security Standards relating to the applications integrated security features. See http://csrc.nist.gov/ for more information.	Source: ; Source Date:	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_012

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.033		To support the Security function, the system must provide the capability to control access to the application, functional modules, transactions, and data by having integrated security features that are configurable by the system administrator.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_013

Chapter	Req Id	Change Type	Requirement	Sources	Treasury's Federal Financial Management Systems Function Guidance (See Appendix A-5)	Treasury's Federal Financial Management Systems Requirement (See Appendix A-5)	DFMIG Rule Name
System Security	14.07.034		To support Security function, the system must provide the capability to maintain general profile identity attributes that could consist of a customer's: • Username; • Name; • Address; • Home telephone number; • Social Security Number; • Date of birth; • Personal e-mail address; • Employer name; • Employer address; • Employee telephone number; • Employer e-mail address; and • Confidential questions and answers.	Source: NISTSP800-53,AppF; Source Date: 4/1/2013	2.4.1.1_Securing Financial Management System Information_P	Provide and monitor Federal information system security controls consistent with information system category (low, moderate, high), impact on security objectives (confidentiality, integrity, availability), and minimum security requirements (for example, access control, configuration management, and incident response) as specified by National Institute of Standards and Technology and consistent with OMB Circular No. A-130.	Revenue_AR_Security_017

ACRONYMS

ANSI	American National Standards Institute
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ATO	Authorization to Operate
CCR	Central Contractor Registration
CFR	Code of Federal Regulations
COTS	Commercial Off the Shelf
DCI	Director of Central Intelligence
DFAS	Defense Finance and Accounting Service
DIACAP	DoD Information Assurance Certification and Accreditation Process
DITPR	DoD Information Technology Portfolio Registry
DoD	Department of Defense
DoDD	Department of Defense Directives
DoDFMR	DoD Financial Management Regulation
DoDI	Department of Defense Instruction
DoS	Department of State
FACTS	Federal Agencies' Centralized Trial-Balance System
FFMIA	Federal Financial Management Improvement Act
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMS	Financial Management Service
FOB	Free On Board
GAO	General Accountability Office
GFRS	Government wide Financial Report System
GL	General Ledger
GOTS	Government Off-the-Shelf
GPEA	Government Paperwork Elimination Act
GTAS	Governmentwide Treasury Account Symbol Adjusted Trial Balance System
GUI	Graphical User Interface
IA	Information Assurance
NAICS	North American Industry Classification System
NARA	National Archives and Records Administration
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSTISSP	National Security Telecommunications and Information System Security Policy
OMB	Office of Management and Budget

OS	Operating System
PDF	Portable Document Format
PKI	Public Key Infrastructure
SIC	Standard Industrial Classification
SQL	Structured Query Language
TAS	Treasury Account Symbol
TCP/IP	Transmission Control Protocol/Internet Protocol
USSGL	United States Standard General Ledger
VPN	Virtual Private Network
WFMC	Workflow Management Coalition
XML	Extensible Markup Language