



ICFS SYSTEM SECURITY PLAN

*HUD Integrated Financial Management Improvement
Project*

U.S. Department of Housing and Urban Development

July 22, 2005



The MIL Corporation

Revision Sheet

Release No.	Date	Revision Description
Rev. 0	06/27/2005	Initial Delivery
Rev. 1	07/22/2005	Final Delivery Incorporating HUD's Comments

U. S. Department of Housing and Urban Development				
Contract Number	C-DEN-01982			
Request Number	R-2004-AY-00378			
Task Number	HIFMIP SDM Define Stage – CDR #26			
Deliverable	ICFS System Security Plan - Final			
Due Date	07/22/2005			
Comments Returned Due Date	08/05/2005			
Comments Returned Date				
Comments:				
Program Area Representative: _____ Mary Kohlmeier			Date: _____	
GTM: _____ Jenny A. Shaker			Date: _____	
GTR: _____ Kenneth Traylor			Date: _____	

**MAJOR APPLICATION
ICFS SYSTEM SECURITY PLAN
TABLE OF CONTENTS**

	<u>Page #</u>
1.0 GENERAL INFORMATION	1-1
1.1 System Identification	1-2
1.2 Purpose	1-4
1.3 System Environment	1-4
1.3.1 Equipment Environment	1-4
1.3.2 Software Environment	1-6
1.3.3 Architecture	1-6
1.4 System Interconnection/Information Sharing	1-7
1.5 Applicable Laws or Regulations Affecting the System.....	1-13
1.5.1 Laws and Regulations	1-13
1.5.2 HUD Security Policies and Guidance.....	1-13
1.5.3 NIST Standards.....	1-14
1.6 General Description of Information Sensitivity.....	1-14
1.7 Points of Contact.....	1-15
2.0 MANAGEMENT CONTROLS.....	2-1
2.1 Risk Assessment and Management	2-1
2.2 Review of Security Controls	2-1
2.3 Rules of Behavior.....	2-1
2.4 Planning for Security in the Life Cycle.....	2-1
2.4.1 Initiation Phase	2-2
2.4.2 Development/Acquisition Phase.....	2-2
3.0 OPERATIONAL CONTROLS	3-1
3.1 Personnel Security	3-1

3.2 Physical and Environmental Protection 3-1

3.3 Production, Input/Output Controls 3-3

3.4 Contingency Planning 3-5

3.5 Application Software Maintenance Controls 3-5

3.6 Data Integrity/Validation Controls 3-6

3.7 Documentation 3-7

3.8 Security Awareness and Training 3-7

4.0 *TECHNICAL CONTROLS* 4-1

4.1 Identification and Authentication 4-1

4.2 Logical Access Controls 4-2

4.3 Public Access Controls 4-3

4.4 Audit Trails 4-3

APPENDIX A - RULES OF BEHAVIOR A-1

APPENDIX B - ICFS INFORMATION SECURITY REFERENCES B-1

LIST OF TABLES

Table 1-1 HUD Target Recommendations – Workstations and Servers 1-5

Table 1-2 HUD Target Recommendations - Storage Devices 1-5

Table 1-3 HUD Target Recommendations – Access Channels 1-5

Table 1-4 HUD Target Recommendations – Operating Systems 1-6

Table 1-5 HUD Target Recommendations – Database Management Systems 1-6

Table 1-6 ICFS Interface Requirements 1-7

Table 1-7 HIFMIP Points of Contact..... 1-15

Table 1-8 HIFMIP MIL Points of Contact..... 1-17

Table 2-1 ICFS Information Security Requirements 2-3

Table 3-1 ICFS Application and Risk Management Documentation 3-7

Table 4-1 HUD Password Policy 4-1

Table B-1 ICFS Information Security Requirements..... B-1

LIST OF FIGURES

Figure 1-1 ICFS High Level Inputs and Outputs 1-3

Figure 1-2 ICFS High Level Systems Architecture Initial Phase 1-6

1.0 GENERAL INFORMATION

1.0 GENERAL INFORMATION

The Department of Housing and Urban Development (HUD) is in the process of modernizing its financial management systems in accordance with a vision of financial management consistent with legislation, OMB directives, modern business practices, customer service, and technology. The overall initiative to implement the financial management vision is the HUD Integrated Financial Management Improvement Project (HIFMIP). Within HIFMIP, several implementation phases have been defined to provide a manageable method of moving from the current state to the desired financial management environment. These phases, as described in the HUD's Financial Management Vision Document (CFO Vision Document) dated June 24, 2005, appear below:

Phase I: Execute a series of short-term improvements to prepare HUD for the implementation of the core financial solution, strengthen financial policy, expedite solution development and select a core solution.

Phase II: Implement an integrated core financial solution that leverages state of the art technologies and reengineers business processes based on federal requirements and industry best practices.

Phase III: Enhance, redesign or replace operational interfaces to eliminate any negative impact on the financial cycle.

Phase IV: Leverage the core financial solution through the implementation of decision support, performance management, and customer relationship management solutions.

Phase II of the HIFMIP project is the implementation of a new HUD-wide financial management system. The new system, currently called the Integrated Core Financial System (ICFS), will provide the first building block to enable later integration with other desired management improvements such as enterprise performance management. HUD describes the end result of the phased approach as the Integrated Financial Management Solution (IFMS), of which ICFS is one key component. HUD is currently preparing to select and implement the ICFS as recommended in the May 18, 2004 Independent Decision and Recommendation Paper (IDRP)¹. The ICFS Security Plan serves the purpose of illustrating the planned security controls that will be inherent in the system.

¹ Calibre, *Independent Decision and Recommendation Paper*, May 18, 2004, rev. June 1, 2004, Section 2.3.2 "Alternative Analysis and Recommendation."

1.1 System Identification

System Name/Title

- Integrated Core Financial System (ICFS) – IAS Code N/A

Responsible Organization

- Office of the Chief Financial Officer (OCFO)

Information Contact(s)

Name: Gail Dise
 Title: Senior Advisor for Financial Systems Project Management
 Address: Headquarters, Room 3220
 Phone: 202) 708-1757 x3749
 E-mail: [Gail B. Dise@hud.gov](mailto:Gail_B._Dise@hud.gov)

Name: Keith Zahner
 Title: Director
 Address: Headquarters, Room 3208
 Phone: (202) 708-1757 x3752
 E-mail: [Keith C. Zahner@hud.gov](mailto:Keith_C._Zahner@hud.gov)

Assignment of Security Responsibility

Name: Jacqueline Rooths
 Title:
 Address: Headquarters, Room 3114
 Phone: (202) 708-1313 x3765
 E-mail: [Jacqueline D. Rooths@hud.gov](mailto:Jacqueline_D._Rooths@hud.gov)

System Operational Status

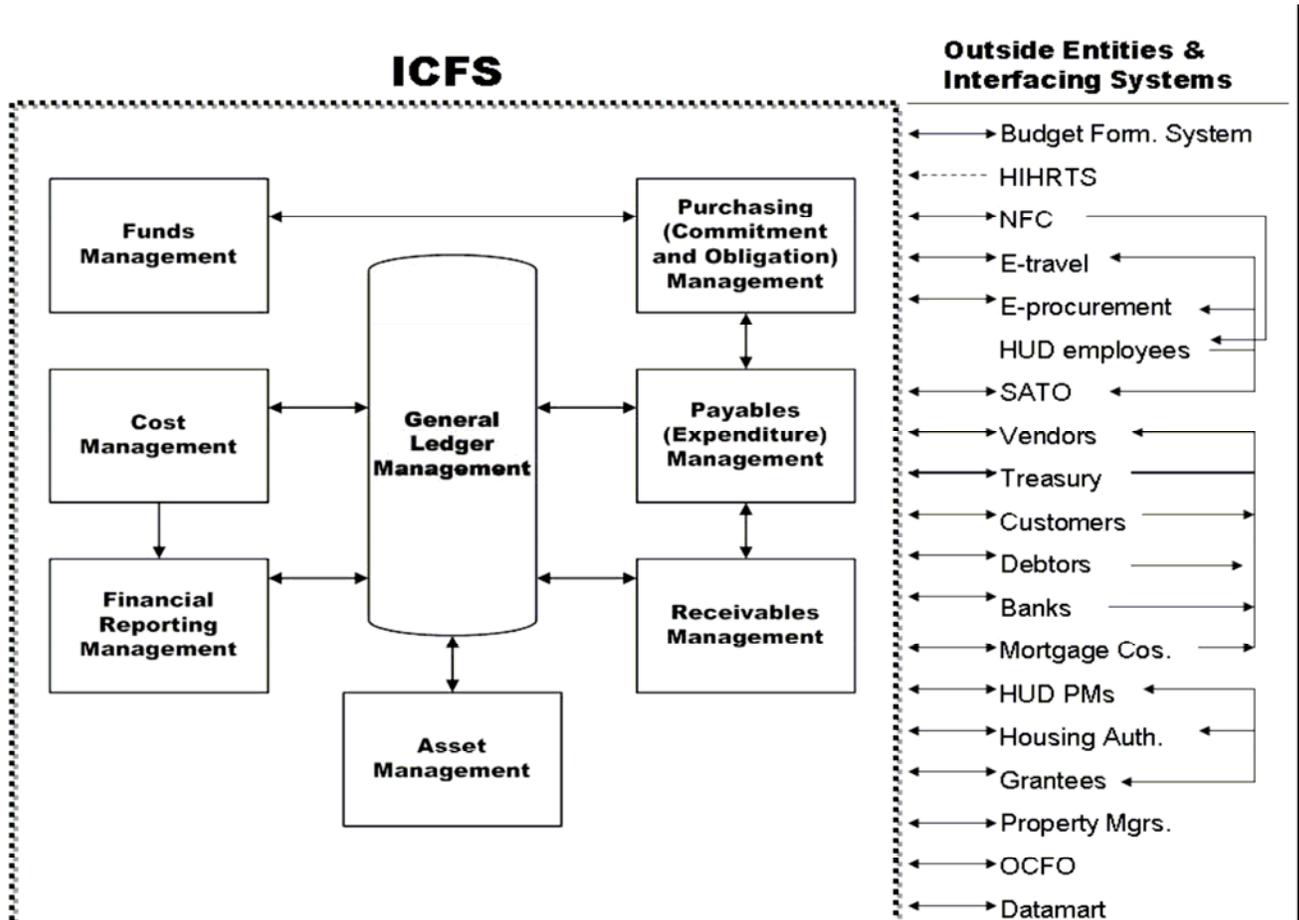
- Under development – Currently in the Definition/Requirements Phase

General Description

ICFS involves the full implementation of an end to end integrated financial system that includes core financial and other functions such as general ledger, accounts payable, accounts receivable, budget execution (funds control), asset management, cost management, reporting, obligation processing, expenditure tracking, acquisition, cash management, cost accounting, financial reporting, workflow automation and federal financial assistance reporting including grants, subsidies and loans. The interfaces will include eTravel, Treasury, payroll, bankcard, and program systems, e.g. IDIS, TRACS. Temporary interfaces until transition to an integrated financial system include FHA Subsidiary Ledger, Ginnie Mae subsidiary general ledger, and OFHEO's Financial Information and Management System (FIMS). The end state broad requirement for HIFMIP is to replace HUDCAPS, PAS, and LOCCS with a modern, compliant, integrated core financial system that will summarize financial data, control funds, prepare annual financial statements, and meet all internal and external reporting requirements across the agency.

ICFS will encompass all HUD financial functions across the programmatic and administrative areas. At a high level, the figure below illustrates the inputs and outputs for the new ICFS.

Figure 1-1 ICFS High Level Inputs and Outputs



The ICFS must support and maintain different business lines for the agency. It is important that the ICFS enforce the validations and rules that exist among and between the business lines. The separate lines of business will be supported in the future state by a single instance of the core financial system running at a Center of Excellence (COE). HUD has developed a definition for the new financial system in the Vision document as:

In accordance with Office of Federal Financial Management (OFFM) (formerly JFMIP), financial management systems must be designed with effective and efficient interrelationships between software, hardware, personnel, procedures, controls, and data contained within the systems. To be integrated, financial management systems must have, as a minimum, the following four characteristics:

- (1) Standard data classifications (definitions and formats) that are established and used for recording each financial event;
- (2) Common processes for similar kinds of transactions;
- (3) Internal controls over data entry, transaction processing, and reporting that are applied consistently; and
- (4) A design that eliminates unnecessary duplication of transaction entry.

See Section 1.7 for list of organizations impacted by the ICFS.

1.2 Purpose

The purpose of the Integrated Core Financial System (ICFS) Security Plan (SP) is to provide an overview of the system security requirements and describe the current management, operational, and technical controls in place or planned for meeting those security requirements. This Plan, in conjunction with the findings and analysis from future Risk Assessments, will provide management with an understanding of the application's security posture. This Plan presents proposed security controls to ensure that the system operates effectively and provides the appropriate level of protection for ICFS data confidentiality, integrity, and availability. The Plan documents ICFS structured approach for security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, unauthorized access to or modification of ICFS information.

The Security Plan is a living document that will be updated periodically to incorporate new and/or modified security controls. The Plan should be revised once the final COTS selection is made as well as when the COE is selected. This Security Plan presents the status of security controls that were in place or planned as of June 27, 2005.

1.3 System Environment

This section presents the technical environment to be used for the commercial off the shelf (COTS) federal financial system for the HUD implementation of the Integrated Core Financial System (ICFS). The environment identified here (and also listed in the Final High-level Functional Requirements Document) is based on the products and specifications identified in the HUD Target Enterprise Architecture v1.0 dated January 24, 2005 and the HUD CIO standards approved by the Configuration Change Management Board (CCMB). Additionally this environment will further comply with the ICFS security requirements that are also addressed in this document. The selection of a COTS federal financial system is in accordance with the provisions of the Clinger-Cohen Act which stipulates that business and information requirements should be met using COTS or government off-the-shelf (GOTS) technologies rather than customized or in-house solutions whenever practical.

This document assumes that the computing environment that this system will reside in has been certified and accredited. If the system is moved to a Center of Excellence (COE), that environment will also be certified and accredited or meet the minimum security requirements as stipulated by the policies and regulations stated below.

1.3.1 Equipment Environment

The equipment required for the ICFS will be dependent upon the specific COTS package selected. The technical architecture of COTS federal financial systems is designed as open systems architecture, allowing its use in a variety of technical environments. This architecture also allows agencies to comply with a variety of enterprise architecture standards. The equipment environment standards presented below are drawn from HUD's Target Enterprise Architecture v1.0.

On-line access to a COTS federal financial system is supported by a workstation able to run a web browser and with access to the HUD standard network. The minimum hardware requirements of a JFMIP-certified, COTS federal financial systems product could be as small as a single hardware server. However, the preferred configuration used in typical production configurations has a dedicated database

server to handle input and output to the backend relational database and one or more application servers dedicated to servicing on-line users and real-time transaction processing from other integrated financial applications. The HUD Target Enterprise Architecture recommends target workstation and server specifications as shown below:

Table 1-1 HUD Target Recommendations – Workstations and Servers

	Target Recommendations	
Service Standard	Products	Specifications
Servers/Computers	N/A	Open Standards (UNIX) Enterprise Server Intel-based server Commodity Intel-based workstation

The capacity of the storage media is dependant on several factors: the size of the operating system and other systems software (for example, middleware and relational data base management systems); the size of the application software and the number of subsystems installed; the amount of historical data to be converted; and, the anticipated years of financial history to be retained. Data storage requirements cannot be determined until the COTS federal financial system has been selected and the design related decisions have been made. HUD’s specification for storage devices is presented in the table below.

Table 1-2 HUD Target Recommendations - Storage Devices

	Target Recommendations	
Service Standard	Products	Specifications
Storage Devices	N/A	Storage-area Network (SAN) Network-attached Storage (NAS)

Access Channels are the interface between the COTS federal financial system and its users. Access Channels can be a web browser, a personal digital assistant or other communication devices. The recommended target products identified in the HUD Target Enterprise Architecture v1.0 is presented in the table below.

Table 1-3 HUD Target Recommendations – Access Channels

	Target Recommendations	
Service Standard	Products	Specifications
Web Browser	Internet Explorer 6.0 Netscape Communicator 4.7	N/A
Wireless/PDA	Palm Pilot V	N/A
Communication/ Collaboration	Lotus Notes/Domino Mail 6.5	

1.3.2 Software Environment

JFMIP certified COTS federal financial systems are supported by a variety of operating systems and relational data base management systems (RDBMS). HUD's standards for operating systems and RDBMS are presented below. If other third party reporting or middleware products are required in the operation of the COTS federal financial system they are usually bundled with the application and will be licensed to HUD on a limited use basis. The CCMB defines HUD's operating system standard.

Table 1-4 HUD Target Recommendations – Operating Systems

Service Standard	CCMB Approved Operating Systems	
	Products	Specifications
Operating System	Windows 2000 Advanced Servers Microsoft Windows XP UNIX Solaris 2.6	N/A

The database management systems recommended for HUD's Target Enterprise Architecture are presented in the table below.

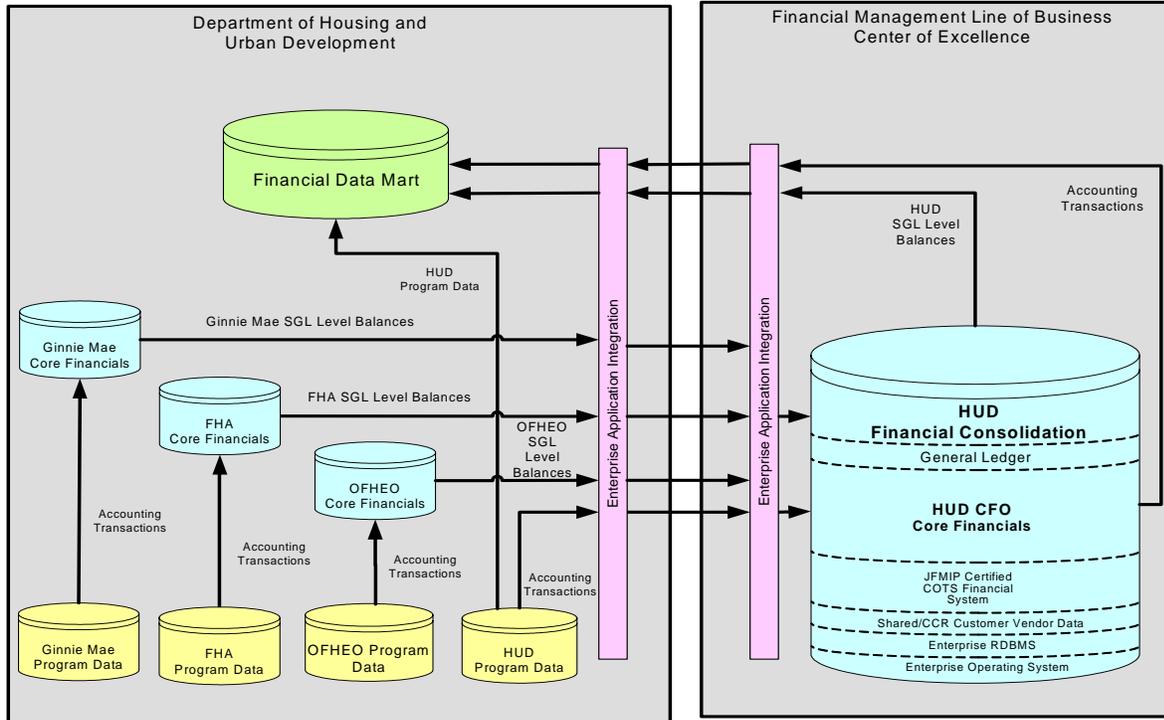
Table 1-5 HUD Target Recommendations – Database Management Systems

Service Standard	Target Recommendations	
	Products	Specifications
Database	Oracle 9i Microsoft Access Microsoft SQL 2000	N/A

1.3.3 Architecture

Figure 1-2 illustrates the proposed system architecture for the initial phase of ICFS. The left side of the diagram details the proposed system architecture for ICFS as managed in a HUD computing environment. Additionally, there is a government-wide initiative to host and manage core financial management functions in a COE environment. This design is illustrated in the right side of the diagram. The minimum security requirements for the COE environment will be stringently expressed in the Service Level Agreement, and should meet, if not surpass the policies and regulations stated in this document.

Figure 1-2 ICFS High Level Systems Architecture Initial Phase



1.4 System Interconnection/Information Sharing

ICFS connects with other HUD systems for the purposes of sharing information resources. The security of interconnected systems is important to ensuring that other systems do not compromise the ICFS application or data. This section of the Security Plan documents the systems planned to interface with the ICFS. Once the COTS selection is made and a COE/Systems Integrator is selected, written authorizations from each of the interfacing systems must be obtained. In addition, Appendix A list the HUD Rules of Behavior which must be followed by every interfacing system to the ICFS.

The table below describes the ICFS interface requirements with internal HUD financial applications and other HUD organizations including the Federal Housing Administration (FHA) and the Government National Mortgage Association (Ginnie Mae).

Table 1-6 ICFS Interface Requirements

Program Office/System	HIFMIP Initial Stage Disposition	Comments/Status
Not Included on A-127 Inventory		
A751 Personal Service Cost Report Subsystem (PSCRS)	- Replace –will include requirements for interfacing from National Finance Center to ICFS.	Process will have to incorporate integration/interface with DOCS information now housed at Treasury

Program Office/System	HIFMIP Initial Stage Disposition	Comments/Status
D51 Departmental Organization Code System (DOCS)	- Interface – to be used in NFC to ICFS interface. DOCS functionality now exists in HIHRTS.	
A75R Financial Data Mart (Financial-DM)	- Interface - Will include requirements for financial information from ICFS for business processes that are changed by ICFS (HUCAPS and PAS) and other ICFS changes.	- Program feeds will remain the same under the Initial ICFS Stage.
A51 Federal Assistance Award Data System (FAADS)	- Interface	
[Unk] Furniture and Equipment Management Information System (FEMIS)	- This is a manual process done once a year. Will include continuing annual manual process.	
[Unk] Financial Information and Management System (FIMS) [OFHEO]	- Replace – Will include OFHEO business processes in FRD requirements	
C48 Home Ownership for People Everywhere 3 (HOPE 3)	- This system has been closed – no action needed	
Office of Administration (4)		
A35 HUD Procurement System (HPS)	- Interface	
D67A Facilities Integrated Resources Management System (FIRMS)	- No current interface or integration with financial system – no action required	
P035 Small Purchase System (SPS)	- Interface	
P-162 HUD Integrated Human Resources Training System (HIHRTS)	<p>- Will interface NFC payroll to ICFS and use DOCS component for organization code conversion</p> <p>- Will interface to ICFS for tracking of security management based on personnel status</p>	

Program Office/System	HIFMIP Initial Stage Disposition	Comments/Status
Chief Financial Officer (17)		
A21 Loan Accounting System (LAS/LASHE)	- Interface financial information to ICFS - Maintain LOCCS interface for payment	
A39 HUD Consolidated Financial Statement System (HCFSS) (Hyperion)	- Replace	
44D Low Rent Housing Security Ledger (SECLEDDGER) Retired 12/10/2004	- No Action	To be closed 1 st Qtr FY 2005 per Keith Zahner e-mail dtd 9/29/04, Subj: FY04 A-127 Self-Assessment Review for CFO systems (PBC item 59).
A65A Section 235 Automated Validation and Editing (SAVE)	- No Action	Interfaces to LOCCS
A67 Line of Credit Control System (LOCCS)	- Interface to/from ICFS	
A75 HUDCAPS/FFS (HUDCAPS)	- Replace	
A91 Consolidated Cost and FTE Files (CCFF)	- Will include functionality in NFC to ICFS interface	
A96 Program Accounting System (PAS)	- Replace	
D08 Bond Payment (BONDMAPPER)	- No Action	Migration to LOCCS by mid-FY2005 per Keith Zahner e-mail dtd 9/29/04
D21 Departmental Accounts Receivable / Collection (DARTS)	- Interface	Manual interface to HUDCAPS
D61 EZBudget Formulation System (EZB)	- No Action - Has no core financial function	No interface to HUDCAPS
D65A Section 8 Budget	- Interface – Receives information from PAS,	Uses budget formulation for

Program Office/System	HIFMIP Initial Stage Disposition	Comments/Status
Outlay Support System (BOSS)	LOCCS, and HUDCAPS	projecting outlays for Section 8. This is where the actual data for the 1 st year of a 3 yr budget is forecasted.
D91A Total Estimation and Allocation Mechanism – Resource Estimation and Allocation Process (TEAM-REAP)	- No Action	
H18 Integrated Automated Travel System (IATS)	- Interface – currently is manual interface	
P001 HUD Travel Management System (HTMS)	- Will interface to new FedTraveler eTravel system	Scheduled to be retired/replaced during the Summer of 2005
Community Planning and Development (3)		
C04 Integrated Disbursement and Information System (IDIS)	- No Action - Has direct interface to LOCCS, then to ICFS	
C38 Special Needs Assistance Program System (SNAPS)	- No Action	
C39 Empowerment Zones/Enterprise Communities Performance Measurement System (EZ/EC)	- No Action	
Office of Housing (20)		
A43 Single Family Insurance System (SFIS)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
A43C Single Family Insurance Claims Subsystem (CLAIMS)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS

Program Office/System	HIFMIP Initial Stage Disposition	Comments/Status
A80B Single Family Premium Collection Sys-Periodic (SFPCS-P)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
A80N Single Family Mortgage Notes Servicing (SFMN)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
A80R Single Family Premium Collection Sys-Upfront (SFPCS)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
A80S Single Family Acquired Asset Management (SAMS)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
D64A SF Housing Enterprise Data Warehouse (SFHEDW)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
F12 Home Equity Conversion Mortgages (HECM)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
F17 Computerized Home Underwriting Mgmt System (CHUMS)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
F31 Cash Control, Accounting and Reporting System (CCARS)	- No Action	Since April 2004 absorbed into PeopleSoft FHA Subsidiary Ledger; the system will remain active until approximately Feb 2005 when the issue of whether or not to keep it active will be addressed. Source: HUD Web CIO Inventory of Automated Systems (IAS)
F42D SF Default Monitoring System (SFDMS)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
F47 Multifamily Insurance (MFIS)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
F51 Institution Master File (IMF)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
F71 Title I Notes Servicing	- No Action	FHA System – not currently linked

Program Office/System	HIFMIP Initial Stage Disposition	Comments/Status
(Debt Collection and Asset Management System (DCAMS))		to HUDCAPS/PAS/LOCCS
F72 Title I Insurance and Claims (TIIS)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
F75 Multifamily Insurance and Claims (MFIC)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
F87 Tenant Rental Assistance Certification System (TRACS)	- Interface financial information to ICFS - Maintain LOCCS interface for payment	
P013 FHA Subsidiary Ledger (FHA-SL)	- Interface	
P057 Multifamily Delinquency and Default Reporting (MDDR)	- No Action	FHA System – not currently linked to HUDCAPS/PAS/LOCCS
Government National Mortgage Association (2)		
B09 Default Management System (DMS)	- No Action	
B16 MACOLA Accounting Software System (MASS)	- Interface	
Public and Indian Housing (3)		
P106 Tenant Eligibility Assessment Subsystem (TASS)	- No Action	
P113 PIH Information Center (PIC)	- No Action	
P181 Enterprise Income Verification (EIV)	- No Action	

All data exchanges must be secure and the system must receive confirmation of completed data transfers.

1.5 Applicable Laws or Regulations Affecting the System

The following laws and regulations establish specific requirements for confidentiality, integrity, or availability of ICFS information. HUD has also followed HUD, OMB, and National Institute of Standards and Technology (NIST) policies and guidelines, listed below, to protect the ICFS system with an adequate level of security commensurate with the level of risk and magnitude of likely harm.

1.5.1 Laws and Regulations

The laws and regulations that apply specifically to confidentiality, integrity, or availability of ICFS information requirements are:

- Federal Information Security Management Act (FISMA), 2002
- The Privacy Act of 1982, Public Law 93-579
- Prompt Payment Act, 1982
- Presidential Decision Directive 63 (PDD-63), Critical Infrastructure Protection, May 1998
- Clinger-Cohen Act of 1996 (40 U.S.C. 1401)
- Department of Treasury, Electronic Authentication Policy, December 2000
- Computer Fraud and Abuse Act of 1986, Public Law, 99-474 (18 U.S.C. 1030)
- Computer Security Act, 1987, Public Law 100-235
- OMB M-00-07, Incorporating and Funding Security in Information Systems Investments
- OMB Circular A-102 - Directive on Cash Management
- OMB Circular A-123 - Directive on Internal Control Systems
- OMB Circular A-125 - Directive on Prompt Payment
- OMB Circular A-127 - Directive on Financial Management Systems
- OMB Circular A-130 - Management of Federal Information Resources
- OMB Memorandum 04-04 – E-Authentication Guidance for Federal Agencies, December 2003

1.5.2 HUD Security Policies and Guidance

HUD complies with the following security policies and guidance to provide an adequate level of security:

- HUD Guidebook to System Development Methodology
- HUD Handbook 2400.24 Rev-2 Information Security Program
- HUD Benefit/Cost Analysis Methodology, Volume 1 – Methodology, Volume II – Workbook (September 1995)
- HUD Handbook 2400.24, Rev. 2, ADP Security Program

1.5.3 NIST Standards

HUD adheres to the following NIST policies and guidelines:

- NIST SP 800-18 - Guide for Developing Security Plans for Information Technology Systems, December 1998
- NIST SP 800-26 - Security Self-Assessment Guide for Information Technology Systems, November 2001
- NIST SP 800-34 - Contingency Planning Guide for Information Technology Systems, June 2002
- NIST SP 800-30 - Risk Management Guide for Information Technology Systems, January 2002

1.6 General Description of Information Sensitivity

ICFS is a major integrated financial system for the Department of Housing and Urban Development. With full implementation, core financial functions plus interface processing with eTravel, Treasury, payroll, FHA Subsidiary Ledger(s), Ginnie Mae subsidiary ledger, OFHEO's subsidiary ledger, and program systems will be stored within. ICFS data will be in use by HUD offices for: planning and managing program activities, evaluating program performance, and depicting financial trends and requirements. The sensitivity level of the system and of the information stored within, processed by, or transmitted by the system reflects the value of the system to the organization and has been used as the basis for implementing the necessary IT security controls for ICFS.

All HUD information can be delineated into two main categories: (1) Public; and, (2) Sensitive. Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to HUD. Sensitive information contains all other non-public information.

Federal IT security standards define the following three basic protection requirements in order to determine the information sensitivity:

1. **Confidentiality** – Protection from unauthorized disclosure
2. **Integrity** – Protection from unauthorized, unanticipated, or unintentional modification
 - a. Non-repudiation – Verification of the origin or receipt of a message
 - b. Authenticity – Verification that the content of a message has not changed in transit
3. **Availability** – Available on a timely basis to meet mission requirements or to avoid substantial losses.

Sensitive information is also categorized by levels to include High (for the most sensitive), Medium, and Low (for the least sensitive). Sensitive data that is classified as 'high' must be protected in a more secure manner than data with a 'low' rating. For example, data protected by the Privacy Act, acquisition actions, and budget information qualifies as highly sensitive data. Security controls must be implemented and tested commensurate with the data sensitivity level.

The core financial system will contain highly sensitive information in all categories. This includes financial data, limited personnel data, vendor/customer data, and control data. It will also contain confidential data concerning Internal Revenue Service 1099 tax records. The sensitivity and criticality of

the information stored within, processed, or transmitted by a system is a major factor in risk management. It will be important to address security requirements effectively while the system is being developed.

1.7 Points of Contact

Government and contractual contacts for the HIFMIP project are listed below.

The HIFMIP HUD Points of Contact below lists the points of organizational contact (POCs) that may be needed by the document user for informational and troubleshooting purposes. The table identifies the type of contact, contact name, department, telephone number, and e-mail address.

Table 1-7 HIFMIP Points of Contact

Type of Contact	Name	Dept.	Telephone	Email
Government Technical Representative	Kenneth Traylor	OCFO	(202) 708-1757 x6241	Kenneth_J._Traylor@hud.gov
Government Technical Monitor	Virginia Shaker	OCFO	(202) 708-1136 x3805	Virginia_A._Shaker@hud.gov
Project Manager	Mary Kohlmeier	OCFO	(202) 708-0614 x3853	Mary_L._Kohlmeier@hud.gov
Business Subject Matter Expert – OCFO Systems	Gail Dise	OCFO	(202) 708-1757 x3749	Gail_B._Dise@hud.gov
Business Subject Matter Expert – Ginnie Mae	Michael Najjum	Ginnie Mae - OCFO	(202) 708-1020 x2344	Michael_J._Najjum@hud.gov
Business Subject Matter Expert – FHA	Ronald Crupi	Housing-Office of Financial Analysis & Reporting	(202) 401-0450 x3371	Ronald_E._Crupi@hud.gov
Macola Project Manager	Wesley Jones	Ginnie Mae Comptroller's Division	(202) 708-4100 x3908	Wesley_E._Jones@hud.gov
FHA-SL Project Manager	William Fuentesvilla	Housing-FHA Comptroller's Office	(202) 708-1020 x2344	William_F._Fuentesvilla@hud.gov
Business Subject Matter Expert	Barbara Dorf	Grants Policy	(202) 708-0667 x4637	Barbara_Dorf@hud.gov
Business Subject Matter Expert – CPD	Laura Marin	Director, Office of Technical Assistance and Management	(202) 708-4604 x4432	Laura_M._Marin@hud.gov
Business Subject Matter Expert – OH	Ronald Spraker	Director, Office of Budget and Field Resources (OH)	(202) 708-8975 x6851	Ronald_Y._Spraker@hud.gov
Business Subject Matter Expert – PIH	Paul Scott	Director, Budget Office (PIH)	(202) 708-0920 x2354	Paul_A._Scott@hud.gov
Business Subject Matter Expert – PD&R	Patrick Tewey	Director, Budget Office (PD&R)	(202) 708-1796 x4098	Patrick_J._Tewey@hud.gov

Type of Contact	Name	Dept.	Telephone	Email
Business Subject Matter Expert – OHHLHC	Michael Hill	Deputy Director (OHHLHC)	(202) 708-0310	Michael_F._Hill@hud.gov
Business Subject Matter Expert – FHEO	Paul Christian	Director, Office of Management and Planning (FHEO)	(202) 708-1009	Paul_T._Christian@hud.gov
Advisory	Hanh Do	IG	(202) 708-0344 x8149	Hahn_T._Do@hud.gov
Procurement Specialist	Michael Mee	OCPO	(303) 672-5281 x1820	Michael_J._Mee@hud.gov
System Owner – HPS, SPS,	Ed Girovasi	ADMN	(202) 708-0294 x7138	Edward_L._Girovasi@hud.gov
System Owner – DOCS	Pauline Figliozzi	ADMN	(202) 708-3452 x3012	Pauline_M._Figliozzi@hug.gov
System Owner – HIHRTS	Barbara Edwards	ADMN	(202) 708-3946	Barbara_J._Edwards@hud.gov
System Owner – HCFSS	Karen Wenstrup	OCFO	(202) 708-1313 x3739	Karen_E._Wenstrup@hud.gov
System Owner – FAADS	Alice Cullom	OCFO	(202) 708-0143 x3754	Alice_B._Cullom@hud.gov
System Owner – CCFF, BOSS	Garland Reid	OCFO	(202) 708-1365 x6822	Garland_J._Reid@hud.gov
System Owner – DARTS	Rudy McKinney	OCFO	(202) 708-0202 x3630	Rudy_V._McKinney@hud.gov
System Owner – IATS	Mary Lou Dominguez	OCFO	(817) 978-5669	Mary_L._Dominguez@hud.gov
System Owner – HTMS	Barry Kahn	OCFO	(202) 708-3154 x6540	Barry_A._Kahn@hud.gov
System Owner – IDIS	Bob Brever	CPD	(202) 708-0790 x4537	Robert_T._Brever@hud.gov
System Owner – TRACS	Lanier Hylton	OH	(202) 708-2677 x2510	Lanier_M._Hylton@hud.gov
System Owner – WASS	Gary Faeth	PIH	(202) 475-8730	Gary_L._Faeth@hud.gov
Acting Director – IT Security	Joyce Little	OCIO	(202) 401-4951 x7404	Joyce_M._Little@hud.gov
System Owner – FIMS	Susan Jacobs	OFHEO	(202) 414-3800	Susan_S._Jacobs@hud.gov
Acting Director – IT Operations	Dennis Peacock	OCIO	(202) 708-0306 x6285	Dennis_M._Peacock@hud.gov
Director, Financial Systems Maintenance and Development Division	Keith Zahner	OCFO	(708) 708-1757 x3752	Keith_C._Zahner@hud.gov
Financial Systems Maintenance and Development Division	Rhonda Press	OCFO	(202) 708-1097 x3774	Rhonda_M._Press@hud.gov

The MIL Corporation points of contact are provided below:

Table 1-8 HIFMIP MIL Points of Contact

Type of Contact	Name	Telephone	Email
Operational Vice President	Linda Glasco	(202) 708-1136 x3814	lglasco@milcorp.com
Project Manager	Karen McGee	(202) 708-1136 x3727	kmcgee@milcorp.com
Quality Assurance Manager/Institutional SME	Mary Ellen Firor	(202) 708-1136 x3835	mfiror@milcorp.com
Institutional SME	David Margolies	(202) 708-1136 x3834	dmargolies@milcorp.com

2.0 MANAGEMENT CONTROLS

2.0 MANAGEMENT CONTROLS

Management controls focus on managing both the application as well as risk. IT Security controls in this category typically require management action for completion, including review and approval of risk and system interconnections, oversight of the system life cycle process to ensure security has been incorporated through each life cycle stage, and periodic evaluations of existing security controls.

2.1 Risk Assessment and Management

A risk assessment is an important tool for the Department's managers to use in evaluating the security of the Information Technology (IT) systems they manage. These assessments are also useful for determining the potential for loss or harm to organizational operations, mission, and stakeholders. The risk assessment provides management with the capability to:

- Ensure IT applications and systems are provided an adequate level of security protection
- Meet Federal requirements for information and system security
- Satisfy oversight organizations
- Establish an acceptable level of risk

Two notable Risk Assessments have been performed that pertain to the ICFS. The first is the HUD E-Authentication Risk Assessment for web-based systems used by external organizations. This assessment provides a general guideline for the auditing of the ICFS once it is implemented since it will be considered a web-based system.

More importantly, a HIFMIP Risk Analysis was performed by an independent IT and Business Process Re-engineering Consulting Organization in April 2004. This Risk Analysis provided details on the overall risks associated with the ICFS implementation. This document is currently being updated and is scheduled for delivery in September 2005.

2.2 Review of Security Controls

Since ICFS is in the Define Stage, a security review cannot occur. While a full assessment of risk may be conducted once the system development is complete, the system will need to comply with the existing HUD assessment standards (such as in the E-Authentication Risk Assessment).

2.3 Rules of Behavior

HUD has created Rules of Behavior that delineate responsibilities and expected behavior of all individuals with access to the ICFS system. The rules state the consequences of unacceptable behavior or non-compliance. The rules of behavior will be available to every user when they access ICFS. All users will be required to acknowledge these rules of behavior prior to being granted access to the system. Thereafter, all users will be required to accept the Rules of Behavior annually or, when the user is granted a higher level of responsibility, whichever comes first. The contents of the rules are attached as Appendix A.

2.4 Planning for Security in the Life Cycle

The ICFS project is currently in the Development/Acquisition phase of the SDLC. Functional requirements have been addressed in the Functional Requirements Document (FRD). In addition, Chapter 7 of the High-Level FRD details the security requirements for the ICFS.

As of April 2005, HUD requires the NIST Security Standards to be incorporated into all System Development Lifecycle (SDLC) planning. The SDM has been updated to reflect the NIST Security Standards. For additional guidance, a detailed list of all applicable policies and regulations are illustrated in Appendix B.

2.4.1 Initiation Phase

The initiation phase involved identifying a need and deciding whether to commit the resources necessary to address the need. This phase is complete for ICFS. HUD realized the need to modernize its financial management systems in accordance with a vision of financial management consistent with legislation, OMB directives, modern business practices, customer service, and technology. Resources have been committed to support the overall initiative to implement the financial management vision through the HUD Integrated Financial Management Improvement Project (HIFMIP).

2.4.2 Development/Acquisition Phase

The ICFS application is categorized as a major financial application system and must conform to both HUD and OMB directives and guidelines concerning security. A major financial application system is defined as one that performs clearly defined functions for a specific group of business users (e.g. HUD OCFO). The ICFS will contain sensitive financial transaction information data, as well as information protected by the Privacy Act. The ICFS will be housed in a yet to-be-determined COE and will be accessed by a large user community throughout HUD and by trading partners. There will be direct data entry by HUD users both at Headquarters and Field Offices and HUD trading partners. There will be incoming and outgoing interfaces in both real-time and batch mode. There is a high level of security risk involved within the system in the areas of availability of system, integrity of data, and confidentiality of data. Since the ICFS will be based on a COTS package, HUD will need to configure the COTS package to meet its security needs. Furthermore, when the ICFS application is installed at a COE, HUD's data must be segregated and secured from other government agencies using the same COE. Personnel from other government agencies cannot be allowed access to HUD's data.

The ICFS will be based on a JFMIP-certified financial system. For this reason, the system should meet the following JFMIP security requirements as they are also required by HUD.

- Have integrated security features that are configurable by the system administrator to control access to the application, functional modules, transactions, and data. The application's integrated security features should be compliant with the National Institute of Standards and Technology (NIST) Security Standards.
- Ensure that the agency's access policies are consistently enforced against all attempts made by users or other integrated system resources including software used to submit ad-hoc data query requests or to generate standard reports.
- Require the use of unique user identifications and passwords for authentication purposes. Passwords must be non-printing and non-displaying. The application must allow 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 and accommodate prohibiting the user from reusing recent passwords.
- Enable the system administrator to define functional access rights (e.g., to modules, transactions, approval authorities) and data access rights (e.g., record, create, read, update and delete) by assigned user ID, functional role (e.g., payable technician) and owner organization.

- Permit the system administrator to assign multiple levels of approval to a single user, but prevent that user from applying more than one level of approval to a given document in order to conform to the principle of separation of duties.
- Allow the system administrator to restrict access to sensitive data elements such as social security numbers and banking information by named user, groups of users, or functional role.
- Maintain an audit logging capability to record access activity including:
 - All log-in/log-out attempts by user and workstation,
 - User submitted transactions,
 - Initiated processes,
 - System override events; and
 - Direct additions, changes or deletions to application maintained data.
- Provide the ability to query the audit log by type of access, date and time stamp range, user identification, or terminal ID.

These requirements were included in the recent Request for Information (RFI) survey of the commercial marketplace. Survey objectives were to facilitate the assessment of technical (including security) and functional characteristics of JFMIP-compliant financial management and related application software currently available.

In addition, a consolidated list of significant security requirements related to the ICFS has been gathered from the NIST, JFMIP, and HUD requirements. They are summarized below.

Table 2-1 ICFS Information Security Requirements

Number / Version	Description	Priority	Verification Method
Authentication			
1 – 1	The system shall utilize Role Based access restrictions. These roles include but are not limited to: OS Administrator, Database developer, Web Application Administrator, and authorized authenticated users	High	Analysis
1 - 2	The system shall have an authorization mechanism in place to control access to system resources and database information.	High	Analysis
1 – 3	The system shall leverage the Enterprise user authentication mechanisms where possible.	High	Analysis
1 – 4	Each access role shall be governed by the Principal of Least Privilege to ensure that users have the least amount of privilege to perform their duties.	High	Analysis
1 – 5	The system shall have separate roles for users from different business areas	High	Analysis
1 – 6	The system shall ensure that business area representatives only have access to their respective business area resources.	High	Analysis
1 – 7	The system shall ensure all machine-to-machine connections are authorized and authenticated.	High	Analysis
1 – 8	The system shall utilize certificate-based	High	Analysis

	authentication for web and network login.		
1 – 9	The system shall restrict access to all ICFS data to authorized users on a need-to-know basis	High	Analysis
1 – 10	The system shall enforce time-out on inactive user connections	High	Analysis
Auditing			
2 – 1	The system shall log all accesses violations.	High	Analysis
2 – 2	The system shall log and monitor changes performed on the system including changes made to user and/or machine privileges.	High	Analysis
2 – 3	The system shall restrict changes to the system logs.	High	Analysis
2 – 4	The system shall log all authorized accesses	High	Analysis
2 – 5	The system shall log all unauthorized access attempts to the system.	High	Analysis
Data Protection			
3 – 1	The system shall utilize encryption mechanisms to transport sensitive system data to users.	High	Analysis
3 – 2	The machine-to-machine connections carrying sensitive data shall be encrypted.	High	Analysis
3 – 3	The system shall isolate data from different business lines and program areas.	High	Analysis
3 – 4	The system shall validate input data prior to committing to database	High	Analysis
3 – 5	The system shall track the origin of updates to the database including, but not limited to source (system process or user account), and date-time tag.	High	Analysis
3 – 6	The system server-components shall be located in an isolated network security zone.	High	Analysis
3 – 7	The Web Application Security Coding Standards shall be used to design and develop the ICFS application.	High	Analysis
3 – 8	All reports and displays containing data from the system database shall be labeled sensitive.	High	Analysis
3 – 9	There shall be an MOU/ISA in place for all external connections to the system.	High	Analysis
3 – 10	A log of changes in user privileges shall be created and maintained.	High	Analysis

3.0 OPERATIONAL CONTROLS

3.0 OPERATIONAL CONTROLS

This section addresses operational security methods and procedures, primarily implemented and executed by people as opposed to systems. Staff in various capacities such as human resources and facilities, protect the HUD systems and data indirectly. Technical support teams maintain technical control and perform specified management activities to ensure system security. Operational Controls include:

- Personnel Security
- Physical and Environmental Protection
- Production Controls
- Contingency Planning
- Application Software Maintenance Controls
- Data Integrity Controls
- Documentation, and
- Security Awareness and Training.

This section describes the operational controls that are in place or planned to meet the protection requirements of the ICFS system and data.

3.1 Personnel Security

HUD's Security Division sets security policy for the Department and is responsible for controlling access to all HUD systems. All new HUD employees and contractors are required to complete HUD Form 22017, Personnel Security & System Access User Registration within 30 days of employment.

Access to ICFS will be restricted by the user's role and responsibilities. All personnel accessing ICFS in the performance of their jobs are expected to read and acknowledge the Rules of Behavior. Failure or refusal to sign the Rules of Behavior can result in immediate termination of the assigned User ID / password. This prevents system access and can result in further disciplinary action as prescribed by the Office of the Inspector General.

3.2 Physical and Environmental Protection

A physical safeguard is any physical means that limits access to data (locked doors, vaults, card/key access).

Dedicated Equipment - If ICFS is hosted within the HUD infrastructure the system should conform to existing HUD IT architecture requirements. Separate operational software and databases will be maintained for production, training, development, and IV&V testing. The production database will be secured behind a firewall. If ICFS is hosted by a COE, the COE would be responsible for ensuring the physical security of the data.

Storage and Protection – HUD staff will be trained to implement procedures to store and protect onsite and offsite materials (software, data, and documentation). The database will be backed up each night by HUD IT personnel. Daily run/log files will be maintained to allow a full recovery up to a point in time during any given day. The nightly backup files will be the basis (point of database initialization) for applying daily updates. Duplicate backups of software and data will be stored off-site. There will be an alternate computer site which has a complete set of back-up software will be available for disaster recovery if the main computer site is compromised. The system capabilities for onsite and offsite storage and protection of materials (software, data, and documentation) will be subject to existing HUD

requirements. Software releases will be under HUD configuration management procedures using PVCS. Input users will be responsible for storage of source documentation based on their program offices procedures.

The following sections are applicable if the ICFS is to be managed at a HUD site. If the software is to be maintained at the COE location, the COE must have similar controls in place.

HUD Computer Center Access (HCC) Controls

If ICFS is to reside at HUD, the building is for the sole support of HUD computer systems and access is restricted to authorized personnel and escorted visitors. HUD production data and systems are supported exclusively at this Lockheed Martin facility.

The main entrance to the center has guards on duty 24 x 7 and additionally has double door security, in which one door must close before the other will open. Other entrance doors have card key access for staff from 6:00 a.m. – 6:00 p.m. weekdays with round the clock video monitoring. In addition, there are fourteen security monitors inside the center and seven monitors outside the center.

The hardware used to develop, test, and operate the system is in a secure area under the control of the Office of Information Technology (OIT). The workstations used to develop and access ICFS are in HUD work areas with limited access. The work areas are kept locked during non-business hours. All environmental controls to protect hardware/software are documented under the General Support Systems Plan.

Headquarters Access Controls

Physical access to HUD Headquarters (HQ) is controlled 24 x 7 by security guards and using a HUD ID badge system. All visitors must have some form of personal identification, wear a visitor's badge, and be escorted by HUD personnel. Metal detectors for personnel screening and x-ray review of packages, briefcases, and other carried items are also used for increased security. Access to select areas within HQ, including server/computer rooms, is restricted by a separate card key system/cipher locks. All wiring closets are locked and access is controlled by the Office of Administrative and Management Services (OAMS).

Fire Safety Factors

The HCC has good fire safety factors in place including: fire/smoke detection devices, water sprinklers and a sophisticated Halon 1301 fire extinguishing system. The Halon system is operational and is professionally checked annually. An alert in the fire detection system automatically notifies the Washington, DC Fire Department.

Failure of Supporting Utilities

The HCC constantly monitors the environmental conditions using DATASITE Environmental Monitoring System and software. The contractor's Operations staff and facility guards are alerted if there are abnormalities in room temperature, loss of power, fire alarm activation, and moisture/humidity discrepancies. This system is tested once a month.

There are nine air handlers to monitor and maintain optimal environmental conditions in the computer room. The computer center itself has an elevated floor (a panel lifter is readily available for access) with water detectors located under the floor. No water pipes are in the vicinity of the computer room. Servers

are supported by Uninterruptible Power Supplies (UPS). UPS batteries are charged constantly and serviced every quarter, as weak cells are found the batteries are replaced.

A backup diesel generator, Caterpillar model 1500kW, is available to provide emergency electrical power for continuous, uninterrupted operations to the computer center only. An automatic transfer switch is installed and if a brown out or black out occurs the generator is started automatically. The generator undergoes a monthly load test. A 2,000 gallon fuel tank will provide approximately 62.5 hours of operation at full load. An Emergency Power Off (EPO) switch is installed at this facility.

Structural Collapse

There is no significant risk of structural collapse at the HCC facility. The architecture of the HUD Headquarters facility holds a majority of the main plumbing lines in the center of the building. Therefore, the fire sprinkler system would be the major concern for water damage to the computer rooms in the event of a false alarm or a smelting electrical fire that might trigger the sprinklers.

Interception of Data

The FTS2001 network has safeguards employed to prevent the interception of data transmission. Protocols used to ensure data integrity are: utilization of secure protocols such as Secure Shell (SSH), Secure Hypertext Transfer Protocol (HTTPS), and Lightweight Directory Access Protocol (LDAP). Secure Socket Layer (SSL) 128 bit encryption/decryption is used to secure data between HUD and HUD Business Partners https connections. HUD is using VeriSign as a certificate authority.

Development Server Room

Production and development servers are kept in separate rooms at HUD HQ. New servers that are added to the development server room are built off-site and brought to HUD. Disconnection of hardware without proper authorization in the development or server room is grounds for suspension of access to the room. Backups of the development servers are done each night by contractor staff.

3.3 Production, Input/Output Controls

Under the current HUD Information Technology Services (HITS) contract, a national Help Desk has been implemented. The Help Desk provides an established and repeatable process for addressing access to HUD applications and systems.

Input into ICFS can either be through direct user input, through integration with other HUD internal and external systems or via data uploads from prepared data input files.

Origin - Input origin is the point at which input data will be collected, prepared, and entered into the system. Information will come into ICFS either through direct on-line data entry by authorized users to data input screens, through real-time interface with HUD internal or external systems, via batch interfaces with HUD internal or external systems or via data uploads from prepared data input files. There will be direct user input of the following types of information:

- Reference information such as accounting classification, posting models and vendor maintenance
- Funds Management
- Purchasing – Commitments and Obligations
- Accounts Payable
- Accounts Receivable

- Cost Management
- Asset Management
- Cash Management
- Grants Management
- Loans Management
- Direct General Ledger Posting and General Ledger adjustments
- Financial Reporting

In addition, there will be interfaces/integration with the following major systems;

- HUD Procurement System (HPS) processes procurements of \$100,000 and over. HPS will send commitment and obligation transactions real-time to ICFS to reserve or obligate funds in the core general ledger. ICFS will send confirmation of transaction acceptance to HPS. This system may be incorporated within ICFS or it may be replaced by a COTS procurement system.
- HUD Small Purchase System (SPS) processes purchases of less than \$100,000. SPS will send obligation transactions real-time to ICFS to obligate funds in the core general ledger. ICFS will send confirmation of transaction acceptance to HPS. This system may be incorporated within ICFS or it may be replaced by a COTS procurement system.
- The replacement for the HUD Travel Management System (HTMS), the HUD eTravel system FedTraveler.com, will provide processing of travel requests and vouchers. FedTraveler will send obligation and payment transactions real-time to ICFS. ICFS will send confirmation of transaction acceptance to FedTraveler.
- The National Finance Center will provide expenditure data on payroll and personnel cost data.
- The Tenant Rental Assistance Certification System (TRACS) provides funds control over Section 8 and other assisted housing programs. TRACS will collect tenant data and automatically provide payment requests for subsidy programs where HUD is the contract administrator based upon the contract and tenant data resident in the system.
- Integrated Disbursement and Information System (IDIS) supports CPD's consolidated planning, disbursement and reporting requirements for the entitlement grant programs (HOME, CDBG, ESG and HOPWA) and simplifies the grants management process for all participants. IDIS also processes contract and payment request information from grantees and controls the payment process.
- Line of Credit Control System (LOCCS) is both a payment tool and a HUD post-award financial grants management system. It is also the link that connects HUD's Program Management Information Systems to HUD's program accounting data. LOCCS is the CFO's primary vehicle for cash management while monitoring grant, loan and subsidy disbursements per the individual control requirements used by HUD's program offices to ensure program compliance.
- Loan Accounting System (LAS) manages loan portfolio system information for the Section 202, Housing for Elderly and Handicapped Loan Program and the Flexible Subsidy program. It is a HUD tool for servicing loans.

Data Entry - HUD personnel will do data entry through a standard HUD desktop workstation with a web connection. ICFS will be accessed by selecting appropriate links from HUD's Intranet or Internet Web pages. HUD trading partners will submit their request for funds electronically or via the Internet. HUD personnel and contractor support staff have an option to access ICFS via either HUD's Intranet or via the Internet (HUD.gov). Both HUD trading partners and recipients will also have the option of using a voice response system for payment requests.

Disposition – Source input such as hard copies of source data entered into the system via data entry screens, interfaces or data uploads should be able to be identified in the system via a document control number or other unique identifier. ICFS security shall comply with the record disposition standards in Handbook 2229.2 Records Disposition Schedule for Automated Systems.

Error Correction – ICFS should be capable of performing data entry edits and validation with ICFS reference information to the extent possible to determine valid data entries and then notify the user with error messages in real-time if needed. Real-time and batch interface processing should provide confirmation/error reports for all transactions processed.

Accuracy and Completeness - At the point of data entry ICFS should provide as much front and back end processing as possible to insure data integrity. Notification to the user should be done in real-time to identify success or failure of input action. Data should not be saved to the system unless it is correct and all required fields are entered. All updates sent to other systems via a real-time or batch interface file should produce a confirmation/error report for all transactions sent and received.

Output control points include:

Production and Distribution - Authorized users, HUD and trading partners, will be able to receive output to their workstation screens, to valid HUD network printers and remote users should be able to direct output to local printers. ICFS shall be capable of transferring files via file transfer protocol (FTP) or Enterprise Application Integration. The system shall be able to accommodate workflow functions including the use of email notification. Besides the interfaces detailed in section 7.2.1.1 Input Control Points there will be the following output only interfaces:

- DARTS establishes and tracks Sec. 236 program collections for Multi-Family Excess Rental Income. DARTS will send collection information to ICFS.
- The Federal Assistance Award Data System (FAADS) gathers information from several Departmental program systems to satisfy a mandate by the Office of Management and Budget (OMB). FAADS data is provided to the Bureau of Census quarterly via FTS file transfer. The ICFS will send obligation and expenditure data to FAADS.

Under the HITS contract, EDS and Lockheed Martin are responsible for the current procedures and processes required to guarantee and protect the application data.

3.4 Contingency Planning

The Federal Preparedness Circular (FPC) 65 provides the guidance to the Federal Executive Branch departments and agencies in the development of viable and executable contingency plans for Continuity of Operations (COOP). HUD has recently developed COOP plans for Headquarters, Regional and Field offices. OSEP is responsible for implementing COOP related actions required for each security threat level.

Disaster recovery/contingency planning includes all procedures necessary to permit HUD to recover from an IT disaster at HQ (e.g., fire in the computer room) or to continue ICFS operations if IT support is interrupted (e.g., failure of hard drive on the physical database server). These two critical components: disaster recovery and response to contingencies will be addressed in the *ICFS Disaster Recovery/Contingency Plan*. This Plan will document the procedures to be followed and the backup process, which ensures a current version of ICFS application software and data are available in the event of an emergency or IT equipment failure. This Plan will work in conjunction with the HUD Continuity of Operations (COOP) plans for Headquarters, Regional and Field offices.

3.5 Application Software Maintenance Controls

Since the ICFS will be based on a COTS package, minimal changes are expected. Nevertheless, software change control processes will be in place to handle modifications or emergency fixes as necessary.

Furthermore, the software vendor will be responsible for providing upgrades and bug fixes. All changes to the software will be documented in designs as well as in updates to user manuals.

Since the software will be housed at a COE, the current plan is for the COE to hold the license for the software. The software is copyrighted by the software vendor.

All software changes will require the approval of the Change Control Management Board. The purpose of the CCMB is to ensure that all changes made to HUD's IT infrastructure or development platforms are done in a rational and orderly process which complies with the goals established in the Clinger/Cohen Act of 1996. The CCMB is chaired by the Director of the Office of Information Technology Operations (OIT). In addition, the CCMB process is intended to:

- Provide the means for interested OIT and CIO staff to comment on proposed changes.
- Document major hardware, software or development process changes in the HUD platforms.
- Provide a central repository of information on changes to the HUD IT infrastructure and system development platforms, including documentation of standard hardware, software and processes.

Change requests can be initiated by any office within IT and the OCIO. The request can be made either on their own behalf or at the request of a program office. No hardware, software or established system development process or standard will be considered Departmental standard until it has been approved by the CCMB. CCMB approval is also required for the one-time use of hardware or software that is not being considered for designation as a Departmental standard. HUD does employ a "Grandfathering" of older software by systems that have been in operation since prior to the implementation of the CCMB.

In reviewing requests to make changes to the established standards, the CCMB will:

- Consider the reason given for making a change to the established platform or for the one-time use of a non-standard product.
- Consider the product or solution that has been proposed as best responding to the need.
- Consider the implementation issues related to the product or solution.

The CCMB will also be the sole authority for declaring that a hardware or software item or a standard development process is no longer a Departmental standard.

3.6 Data Integrity/Validation Controls

ICFS must maintain data integrity. Integrity controls are used to protect the operating system, applications, and information transmitted from the ICFS to the COE from accidental or malicious alteration or destruction. These controls provide assurance that data meets expectations relative to quality and that the data has not been altered by unauthorized means. The risk and magnitude of harm that could result from unauthorized modification of ICFS data is rated as high. The loss of integrity can be the result of intentional (e.g. fraud, abuse) and unintentional acts (e.g., mistakes, errors, and omissions).

Integrity controls from both an ICFS and COE perspective include antivirus software, complex password protection, intrusion detection, performance monitoring and periodic penetration testing. These are essential in maintaining all data and system integrity.

Integrity controls include:

- Anti-Virus Software – HUD currently employs McAfee VirusScan Enterprise 8.0i
- Reconciliation Process – There are specific times throughout the fiscal period when reconciliation activities take place to ensure data consistency between subsidiary modules and the general ledger

- Intrusion Detection – Network safeguards employed at HUD are Secure Shell, Secure Hypertext transfer Protocol, and Lightweight Directory Access Protocol. For password synchronization, HUD uses PassGo Single Sign-on.

Another method for insuring data integrity is having security profiles that define data entry and data update capabilities for a given user role. Personnel will be assigned to a given user role/security profile. As appropriate, data entry will be oriented to and controlled by pop-up lists and threshold controls which identify valid values for a given data field. HUD personnel with data update authority will be required to have a limited background investigation to help identify persons who may represent unacceptable risks for controlling sensitive information.

3.7 Documentation

Documentation includes specific documents developed by HUD as part of the systems development life cycle. Examples of such documentation include: standard operating procedures (SOPs) and security documentation. Other documentation includes vendor supplied documentation for hardware and commercial software. A list of the documents with completion status is provided in the table below.

Table 3-1 ICFS Application and Risk Management Documentation

Document Name	Status
Database Architecture	Complete
Functional Requirements	Complete
Interface Document	Planned
System Design	Planned
System Test Plan	Planned
ICFS User Rules of Behavior	Complete
Configuration Management Plan	Planned
HUD Disaster Recovery Plan	Planned
Memorandum of Understanding (MOU)	Complete
Certification and Accreditation Statements/Documents: Risk Assessment Report (includes Risk Management Plan), Security Test and Evaluation Report	In Progress
ICFS Disaster Recovery/Contingency Plan	To Be Determined
ICFS System Security Plan	In Progress

3.8 Security Awareness and Training

The application rules of behavior are the primary mechanism for application-specific security awareness and training. The rules define the users' expected behavior for the protection of data confidentiality, integrity and availability. Additionally, the rules define expected behavior in terms of protecting the

application, data, and operational platform from damage due to introduction of malicious code, password compromise or disclosure, and use of unauthorized accounts. These rules will be made available to ICFS users prior to obtaining system access and all users are forced to acknowledge acceptance of the rules to have continued access to the application. Users must reaccept these rules on an annual basis. The rules apply to all users authorized to access ICFS, including users from external organizations, such as Ginnie Mae, FHA, and OFHEO.

Additional security awareness and training, while not application specific, is provided annually for general HUD staff and HUD-internal contractor development and support staff. The general training provides the foundation that HUD staff and contractor development and support staff need to fully understand the scope of their security responsibilities and potential impact of security compromise on any HUD application. General security awareness and training addresses the “why should I do/not do this” and provides an additional layer of assurance that staff with critical ICFS development and operational functions are trained to fulfill security responsibilities that will directly or indirectly protect ICFS code, data, and ongoing operations.

4.0 TECHNICAL CONTROLS

4.0 TECHNICAL CONTROLS

This chapter addresses technical controls relative to identification and authentication, logical and public access controls, and audit trails.

4.1 Identification and Authentication

Below is the HUD policy on passwords. It is contained in the HUD Handbook, which is currently undergoing validation and approval.

Table 4-1 HUD Password Policy

HUD Policy	
1.	In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce appropriate measures to ensure that strong passwords are used.
2.	In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce the appropriate frequency for changing passwords; but in no case shall the frequency be less often than every 90 days.
3.	Users shall not share personal passwords.
4.	Users shall select strong passwords and not reuse old passwords.
5.	Use of group passwords shall be limited to situations dictated by operational necessity or those critical for mission accomplishment. Use of a group USERID and password must be approved by the appropriate Authorizing Official.
6.	In those systems where user identity is authenticated by password, the system shall ensure that users cannot reuse a password for at least eight iterations.
7.	In those systems where user identity is authenticated by password, the system shall ensure that passwords are not displayed when entered.
8.	In those systems where user identity is authenticated by password, the system shall protect passwords from unauthorized disclosure and modification when stored and transmitted.
9.	System administrators shall replace all default passwords provided by the vendor.
10.	In those systems where user identity is authenticated by password, the system ISSO shall develop and implement administrative procedures for initial password distribution, for lost/compromised passwords, and for revoking passwords.

Passwords must be changed every 90 days. The password is associated with a single user ID that is assigned to a single individual. The passwords are encrypted and stored to be used to validate against reoccurring passwords. If a password has expired or is forgotten/lost, resets are obtained through the National Call Center.

If more than three invalid login attempts occur, the User ID is disabled and can only be reset by calling the Help Desk.

4.2 Logical Access Controls

The various access controls for the ICFS application cannot be fully defined until the application is selected. However, HUD procedures and standards will pertain regardless of the new application.

HUD grants ICFS access based upon job responsibility. HUD user authentication for LAN/WAN rules will specify that passwords shall be suspended after 45 days of no activity and removed after six months of no activity. The COTS package will control access by application window. The ICFS will be based on a JFMIP certified financial system. It is assumed that the system will meet the following JFMIP security requirements for access control.

- Have integrated security features that are configurable by the system administrator to control access to the application, functional modules, transactions, and data. The application's integrated security features should be compliant with the National Institute of Standards and Technology (NIST) Security Standards. (JFMIP TH-01)
- Ensure that the agency's access policies are consistently enforced against all attempts made by users or other integrated system resources including software used to submit ad-hoc data query requests or to generate standard reports. (JFMIP TH-02)
- Require the use of unique user identifications and passwords for authentication purposes. Passwords must be non-printing and non-displaying. The application must allow 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 and accommodate prohibiting the user from reusing recent passwords. (JFMIP TH-03)
- Enable the system administrator to define functional access rights (e.g., to modules, transactions, approval authorities) and data access rights (e.g., record create, read, update and delete) by assigned user ID, functional role (e.g., payable technician) and owner organization. (JFMIP TH-04)
- Permit the system administrator to assign multiple levels of approval to a single user, but prevent that user from applying more than one level of approval to a given document in order to conform to the principle of separation of duties. (JFMIP TH-05)
- Allow the system administrator to restrict access to sensitive data elements such as social security numbers and banking information by named user, groups of users, or functional role. (JFMIP TH-06)
- Maintain an audit logging capability to record access activity including:
 - All log-in/log-out attempts by user and workstation,
 - User submitted transactions,
 - Initiated processes,
 - System override events; and

- Direct additions, changes or deletions to application maintained data. (JFMIP TH-07)
- Provide the ability to query the audit log by type of access, date and time stamp range, user identification, or terminal ID. (JFMIP TH-08)

4.3 Public Access Controls

While one of the requirements for the new financial application is for it to be web-enabled, the application will only be available on the HUD intranet. Therefore, the public will not have access to ICFS.

4.4 Audit Trails

The ICFS will have the capability to create and maintain a journal file of all accounting events that will affect general ledger and funds control changes. It will also be able to create a transaction audit file that will record all additions, updates, and deletions to designated reference information along with any attempts to perform these actions. This will be in addition to any monitoring and auditing functions performed at the operating system level. Once an entry is made to the journal or transaction audit file it will not be able to be modified or deleted from those files.

The industry standard for security audits is every 90 days. Auditors have looked unfavorably on applications, systems, and agencies that do not maintain a repeatable, logical and definable audit process. Audit trails will be provided in the system to track on-line or batch changes to the system. Any additions, changes, or deletions to records in the system will be tracked in the audit trail. The audit trail will contain, at a minimum, the following fields:

- Table ID
- Key record information
- “Before” data
- “After” data
- User id
- Date
- Time

Additional audit trails, not security-related, will be maintained in the ICFS. For example, ICFS must be able to summarize general ledger entries to create trial balances at different levels. Summaries should be provided by:

- Accounting period (e.g., month and fiscal year)
- General ledger account
- Budgetary accounting information (e.g., division, organization, etc)
- Appropriation

The ICFS must also be able to decompose a general ledger balance down to the individual transactions that created the balance. Due to the importance of journal entries, all detail journal entries must be available for online querying and reporting for the current open year. Once the fiscal year has been closed and all reports have been verified and delivered, detailed entries may be stored offsite.

The transactions that created the entries can be archived once the transaction has been accepted and has successfully updated the database. The results of the transactions (other than journal entries) should be

maintained for a period of 5-7 years depending on the longevity of the appropriation that was referenced by the transaction.

APPENDICES

APPENDIX A - RULES OF BEHAVIOR

Rules of Behavior for Chief Financial Officer Major Application Systems

The Office of the Chief Financial Officer (CFO) may grant system access to employees, contractors, clients/customers, and program participants who have a need to utilize CFO major application systems. These include: HUD's Central Accounting and Program System (HUDCAPS/FFS), Line of Credit Control Systems (LOCCS), Program Accounting System (PAS), Departmental Accounts Receivable Tracking/Collection System (DARTS), and Loan Accounting System (LAS).

Access to the CFO's major application systems is **for official use only**. The system user identification (User ID) and password issued to you are to be used solely in connection with the performance of your responsibilities in support of the HUD mission and may not be used for personal or private gain. As a condition of receiving access, you agree to be responsible for the confidentiality of the assigned information and accountable for all activity with your user identification (User ID). Further, you agree that you will not provide this confidential User ID/ password to anyone, and that you will notify the CFO Security Office upon leaving the employment of your existing office and/or the Department.

Additional rules of the system follow:

- a) Log off the system when leaving the system/workstation area.
- b) Refrain from leaving written passwords in the workstation area.
- c) Passwords for application systems must be changed periodically, and the rules for length, composition (uppercase/lowercase, numeric) and reuse are dependent on individual application controls.
- d) Your User ID will be suspended after 45 days of inactivity and you will need to contact the Information Security staff at 202-708-3300 (Option 3) for a password reset.
- e) Your User ID will be terminated after six months of inactivity, and you will need to re-apply for access to the system.
- f) Avoid posting printouts of sensitive output data on bulletin boards.
- g) Avoid leaving system output reports unattended or unsecured.
- h) Control input documents by returning them to files or forwarding them to the appropriate contact person in your office.
- i) Avoid violation of the Privacy Act, which requires confidentiality of personal data contained in government and contractor data files.
- j) Report security violations immediately to the CFO Security Office at 1-877-705-7504, or the Government Technical Representative (if you are a contractor).
- k) Cooperate in providing personal background information to be used in conducting security background checks required by Federal regulations.
- l) Respond to any requests for information from either the Government Technical Representative, CFO Security Office or management officials regarding system security practices.
- m) Review the Department's "Information Security Guide" and other security guidance at: <http://hudweb.hud.gov/po/i/it/security/gensec.htm>.

Actions violating any of these rules will result in immediate termination of your assigned User ID/ password from the system and can result in further disciplinary action as prescribed by the Office of the Inspector General.

CERTIFICATION: I have read the above statement of policy regarding system security awareness and practices when accessing HUD's information resources. I understand the Department's policies as set forth above, and I agree to comply with these requirements as a condition of being granted limited access to the CFO's information technology resources.

System User's Name (print)

System User's Name (signature)

Date

APPENDIX B - ICFS INFORMATION SECURITY REFERENCES

Error! Reference source not found. summarizes the laws, regulations, HUD policies, and NIST guidance used to develop the security requirements in this document.

Table B-1 ICFS Information Security Requirements

Policy Compliance				
Laws and Regulations	<ul style="list-style-type: none"> Federal Information Security Management Act (FISMA), 2002 The Privacy Act of 1974, Public Law 93-579 Presidential Decision Directive 63 (PDD-63), Critical Infrastructure Protection, May 1998 Clinger-Cohen Act of 1996 (40 U.S.C. 1401) Department of Treasury, <i>Electronic Authentication Policy</i>, December 2000 Computer Fraud and Abuse Act of 1986, Public Law, 99-474 (18 U.S.C. 1030) OMB M-00-07, Incorporating and Funding Security in Information Systems Investments OMB Circular A-102 - Directive on Cash Management OMB Circular A-123 - Directive on Internal Control Systems OMB Circular A-125 - Directive on Prompt Payment OMB Circular A-127 - Directive on Financial Management Systems OMB Circular A-130 - Management of Federal Information Resources 	High	Analysis	
HUD Security Policies and Guidance	<ul style="list-style-type: none"> HUD Guidebook to System Development Methodology HUD Handbook 2400.24 Rev-2 Information Security Program HUD Benefit/Cost Analysis Methodology, Volume 1 – Methodology, Volume II – Workbook (September 1995) HUD Handbook 2400.24., Rev. 2, ADP Security Program 	High	Analysis	
NIST	<ul style="list-style-type: none"> NIST SP 800-18 - Guide for Developing 	Medium	Analysis	This rating is

Standards	Security Plans for Information Technology Systems, December 1998 <ul style="list-style-type: none">• NIST SP 800-26 - Security Self-Assessment Guide for Information Technology Systems, November 2001• NIST SP 800-34 - Contingency Planning Guide for Information Technology Systems, June 2002• NIST SP 800-30 - Risk Management Guide for Information Technology Systems, January 2002			medium due to the fact that the NIST publications only provide guidance.
------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--------------------------------------------------------------------------