DETAIL-LEVEL FUNCTIONAL REQUIREMENTS DOCUMENT

HUD Integrated Financial Management Improvement Project

U. S. Department of Housing and Urban Development

August 9, 2005

The MIL Corporation

Revision Sheet

Release No.	Date	Revision Description
Rev. 0	06/27/2005	Draft Detail-level Functional Requirements Document submitted
Rev. 1	07/26/2005	Incorporated comments from Deliverable Acceptance Report dated July 12, 2005
Rev. 2	08/09/2005	Incorporated additional HUD comments from Deliverable Acceptance Report dated August 4, 2005

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 #10			
Deliverable	FINAL Detail-level Functional Requirements Document			
Due Date	08/09/2005			
Comments Returned Due Date				
Comments Returned Date				

Comments:

Program Area Representative: _Mary Kohlmeier ____________________________ Date: ________

GTM: __________Jenny A. Shaker____ Date: ________

GTR: ___________Kenneth Traylor____ Date: ________

FUNCTIONAL REQUIREMENTS DOCUMENT

TABLE OF CONTENTS

Page #

7.0   SECURITY

7.0 SECURITY

The Integrated Core Financial System will be a HUD enterprise-wide solution based on a JFMIP approved COTS software package. The enterprise-wide COTS package will support the transaction processing and/or consolidation of financial transactions from HUD, OFHEO, FHA, and Ginnie Mae. As HUD's core financial system, it is considered critical to the Department's federal role, and must be protected from loss of data, unauthorized alteration of data, cessation of service, or revealing sensitive information to unauthorized persons. Due to the sensitive nature of the financial information that will exist in the new system, appropriate security features must be in place. This section of the Detail-level FRD describes the security control points, vulnerabilities, safeguards, system monitoring and auditing requirements for the proposed system at a high level. A more detailed description of security requirements will be provided in the System Security Plan.

7.1 Background Information

7.1.1 Background Information on the Sensitivity and Classification of the Application

The current HUDCAPS and supporting financial systems security structure is based on user IDs and passwords. A user must have a valid user ID and password that allows them to access the HUD network and a user ID and password for the applicable financial system. The user must initially successfully log on to the HUD network before a financial system session can be established. Then the user initiates a session with the applicable financial system. Each of the current financial systems maintains its own security protocols and valid user id and password combinations. These user id and password combinations require periodic password changes. The user ID will also be suspended after a HUD prescribed number of days pass without being active. A financial system user ID has one of three access levels assigned to it: view only, modify only, or view and modify combination. The systems access can be limited by type of transaction being viewed/processed, type of data being viewed including Privacy Act information, and the type of modification being performed.

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 HUD's 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 normal ICFS availability will be during HUD normal business hours. There will be time periods, such as at the end of the fiscal year that the system will need to be available during extended business hours. Sections of the system, such as payment request capability, will need to be available 24-hours/7-days a week – with reasonable response time. The possible magnitude of harm that could result from the system not being available to use, or too slow to use effectively, is rated as high. The risks of unavailability of the system must be offset with safeguards that address hardware/software failures, system disruptions, virus attacks, and national disasters. The lack of system responsiveness may be caused by such factors as insufficient hardware, configuration issues, or too many users for the design of the system. Any downtime, particularly during normal working hours, will impact the completion of work and may cause work stoppages in some cases. ICFS must be implemented with a high degree of availability (e.g., hardware redundancy and backup) and it must have executed the required Contingency/Backup Plan to guard against extended down time.

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). Other 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. Another method for insuring data integrity is having security profiles that define for 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.

7.1.2 JFMIP Core System Security Requirements

The ICFS will be based on a JFMIP certified financial system. It is assumed that the system will meet the following JFMIP security requirements. These requirements 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. (JFMIP TH-01)
- Ensure that the agencies 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., system accountant) 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)

7.2 Control Points, Vulnerabilities, and Safeguards

7.2.1 Control Points

A control point can be located at any interface at which there is a movement of data within or between sites. The following section describes the high level input, process, and output control points that have been identified as areas where security vulnerabilities may occur. Input and output into and out of ICFS can be through direct user interface or through integration with other HUD internal and external systems. Input, process and output control points have been identified as areas where security vulnerabilities may occur.

ICFS will limit input based on user access profiles that are stored and maintained within the ICFS security database entity/attribute structures. ICFS access controls will not be oriented solely to Create, Read, Update, and Delete designations but security will be oriented to and checked against a users rights to given organizational information. Menus will be tailored to reflect options that are available to the given user type. Data selections from menus for query, update, and reporting will be limited to those associated with user type and those granted in the user's security access profile for a given organization. User controls will be established so that there will be separation of duties as prescribed by standard accounting practices and procedures. After 21 days the ICFS will require the password to be changed.

ICFS must maintain security and data integrity by allowing only users who possess valid combinations of User Ids and Passwords to access the system. Also ensure that the ICFS is inaccessible after a specified number (normally three) of unsuccessful logon attempts for invalid logon ID or password. The users, whether HUD staff or trading partner, are allowed access to only those financial functions that have been requested and approved by the Security Administrator. In addition, ensure that users are deactivated after a specified period of account inactivity (e.g. user does not log on for ninety-one days). HUD data at a COE must be segregated and secured from other government agencies' data. HUD user's access must be distinguished by profile and/or security ID from these other agencies to ensure data is being accessed and modified by those with the proper authority to do so and not co-mingled with data and confidential information from other agencies using the same COE.

7.2.1.1 Input Control Points

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 ICFMS 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) is the HUD eTravel system FedTraveler.com; and 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. LAS is currently being replaced by a COTS software package.

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.

7.2.1.2 Process Control Points

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.

System Interface - ICFS will have many links with other HUD systems, other government systems and with trading partner systems. These interfaces are listed in section 7.2.1.1 Input Control Points and 7.2.1.3 Output Control Points.

7.2.1.3 Output Control Points

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.

7.2.2 Vulnerabilities

ICFS is vulnerable to input error, loss or compromise of information or denial of service. The ICFS will be an enterprise wide system with internal and external users. ICFS will be receiving and sending data/information to other HUD systems and trading partners. Erroneous data may be entered at any of the input/output points described in section 7.2.1. Vulnerabilities include:

- Access controls will not be sufficient to protect privacy.
- Update controls will not be sufficient to safeguard reliability and integrity.
- Controls to prevent the co-mingling and access of data between federal agencies sharing the same COE will not be sufficient to safeguard privacy and accuracy of information.
- Internet environment may not be appropriate for controlling sensitive payment transactions due to the level of security and controls of the web based COTS financial systems. Further research will be required after product selection to confirm the level of security, and additional security and controls may be warranted.

However, ICFS will have online and interface edits to validate transactions before they are accepted by ICFS. ICFS will be a JFMIP COTS certified system. The JFMIP testing process has vetted the COTS systems to reduce security vulnerabilities. If HUD chooses to use a Center of Excellence service provider, HUD must verify the service provider’s security protocols are to HUD standards.

7.2.3 Safeguards

In order to reduce security vulnerability at each control point certain safeguards can be taken to minimize the risks.

7.2.3.1 Administrative Safeguards

An administrative safeguard is defined as any procedure that requires management supervision.

Personnel - All users who will update ICFS must have passed a standard HUD security and background screening. When users leave HUD or transfer to other positions, procedures will be in place to close user account access as needed. Customers will be required to affirm that they will follow HUD Security procedures and policies including rules of behavior. OCFO will require persons who are authorized ICFS access to periodically re-certify the continued need for system access. Customers must be re-certified every 6 months. HUD staff and contractors will be re-certified every quarter. The production database will not be accessed by software development personnel unless specifically authorized by the system sponsor.

Security Awareness and Training - The Computer Security Act requires federal agencies to provide mandatory, periodic training in computer security awareness and accepted computer security practice for employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of a federal agency. The requirement includes contractors and agency employees. OMB Circular A-130, Appendix III, which was issued in 1996, enforces such mandatory training by requiring its completion before access to the system is granted and through periodic refresher training for continued access. Therefore, each user must be versed in acceptable rules of behavior for the system before being allowed access to it. The training program also should inform users how to seek help when having difficulty using the system and of procedures for reporting security incidents.

Access provided to members of the public should be constrained by controls in the applications, and training should be within the context of those controls and may only consist of notification at the time of access.

Contractor employees are required to receive the same level of automated information systems security awareness and training as federal employees.

Collection and Preparation - Critical functions will be divided among individuals, promoting separation of duties and internal controls. Primary and back-up personnel should cover key positions. Data backup should be part of the Computer Operations group's daily procedures. Data backup testing and validation should be part of the computer operations group's daily procedures.

Environmental Constraints - The ICFS should be available to users 24 hours a day, 7 days a week (24 x 7) except for interruptions for software installation periodic cycles, hardware maintenance or unplanned outages due to hardware, software, or network problems.

Distribution - Standard HUD distribution procedures will apply to any reports produced by this system. The system should be capable of producing interface files in formats acceptable to receiving HUD systems.

Access/Permission - Standard HUD security forms and procedures will apply for allowing users access to this system. ICFS will have administrative safeguards that reinforce security awareness, assist users to determine if their user ID has been possibly compromised, and limit screen options to those defined within the User ID's security profile. ICFS will use the user profile/user class concept to group user access/permissions.

7.2.3.2 Physical Safeguards

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

Dedicated Equipment - Section 5 Environment describes ICFS' equipment needs. 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.

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 available for disaster recovery if the main computer site is compromised. These safeguards also apply when considering a COE and what the contingency plan is for protecting and restoring, if necessary, multiple data sets from a variety of government agencies. 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.

7.2.3.3 Technical Safeguards

A technical safeguard is defined as any automated process that assures appropriate processing (passwords, read/write keys).

User Access - The system should be able to provide restricted access based on the user's access. The user's access will restrict the type of information the user sees, the transaction processes the user can enter and/or approve and the reports and data on the reports the user runs. Security administrators should be able to create and modify user access writes. User-ids and passwords will be issued and controlled following HUD OCIO Security procedures and policies for both internal and Web access. Web user-id authentication and access approval will comply with HUD requirements and be compatible with Web authentication software in use by HUD, such as Lightweight Directory Access Protocol (LDAP). LDAP software will be used to provide Internet security for external users (outside HUD's firewall). LDAP is a software protocol that is an industry standard for "authentication" services, so that web, email, and file sharing servers can use a single list of authorized users and passwords.

Single Sign-on (SSO) controls will be used by ICFS for Intranet and system access. SSO software controls the system's user ID and Password. Passwords must be at least 6-characters comprised of at least one number and at least one uppercase letter. SSO does NOT have time-out controls for extended non-use periods. Hence, ICFS must control time-outs after 60 minutes of inactivity.

Process Safeguards - The system should have the capability to provide data encryption for tables or fields selected by user, such as password encryption.

Security Identification Requirements - None identified

7.3 System Monitoring and Auditing

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.

7.3.1 Journalizing

Journalizing is the recording of selected events as they occur within the system. Journalizing provides the basis for monitoring the processing and use of data and the use of computer resources.

The ICFS must include detail journals for all transactions that occur in the system. A general journal will be kept that will contain each debit and credit transaction that occurs. Optionally, memo journals can be kept to track additional entries that aren’t necessary for the general ledger.

7.3.1.1 Triggering Criteria

Entries will be created in the general journal when a transaction is accepted (without hard errors) in the ICFS. Any time a General Ledger account is updated, a journal record will be created.

7.3.1.2 Identification Information

Each record in the journal will contain, at a minimum, the following identification information for the entry:

- Date
- Time
- User
- Terminal identification
- General Ledger account
- Transaction ID (Document ID)

- Transaction Code
- Transaction Type

7.3.1.3 Application Data

Each record in the journal will contain, at a minimum, the following application information for the entry:

- General Ledger account
- Dollar amount
- Accounting strip information (including Division, organization, appropriation, program, etc.)

7.3.1.4 Journal Use

The journal will be used as the primary basis for reporting since it will contain detail general ledger updates. Since the journal is critical, automated system assurance reports should be included to verify that the journal is being updated properly. For example, reports should verify that debits equal credits for all records in the journal. Reports should also verify that all on-line and batch transactions that have occurred in the system that day have a corresponding record in the general journal for that day.

7.3.2 Audit Trail

In addition to the general journal, audit trails will be provided in the system to track other 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
- Transaction code
- Transaction type
- “Before” data
- “After” data, including what fields from the tables were posted.
- User id
- Date
- Time

When considering a COE service provider, the provider will need to maintain the integrity of the audit trail between the general ledger and tables.

7.3.2.1 Transactions Back to Original Source Documents

For ICFS, transactions will be tracked back to their original source document. Based on the stakeholder requirements, the system will enable the user to identify the source of all data recorded in the system; including standard and user friendly tracking mechanisms employed to enable the tracing of transactions back to its source. Since tracking is desired, naming conventions can be used for Transaction Ids.

7.3.2.2 Transactions Forward to Summary Totals

The ICFS must be able to summarize general ledger entries to create trial balances at different levels. Summaries should be provided by:

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

7.3.2.3 Summary Totals Back to Component Transactions

The ICFS must also be able to decompose a general ledger balance down to the individual transactions that created the balance.

7.3.2.4 All Record Disposition Schedules

Due to the importance of the journal entries, all detail journal entries must be available for online querying and reporting for the current open year and the prior fiscal 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 the required retention period appropriate for the type and purpose of the document. The retention periods for financial records have been established by GAO and retention periods for non-financial records have been established by the National Archives and Records Administration.