Office of Federal Housing Enterprise Oversight (OFHEO)

Technology and Information Management Five Year Strategic Plan

FY 2007 - 2011

Approved: _____ **Date:** 6/27/07

FOREWORD FROM THE CHIEF INFORMATION OFFICER

As the safety and soundness regulator of two of the world's most financially complex institutions, OFHEO has made investments in information technology that are different from most other regulators. Some of these investments stem from the specific legislation that originally created the agency and its capital classification process and risk-based capital model. Other investments such as in the agency's automated supervisory tool (xWorks) were made to provide supervisory tools to effectively support the assessment of the controls and processes of the two regulated Enterprises. Historically the bulk of the agency's systems were acquired or developed separately by the various program offices. This resulted in the development of different processes for acquiring, developing, maintaining, and supporting the agency's information technology investments. An Investment Review Board was created to make the acquisition process consistent across the agency.

The information technology challenge before the agency is to move towards a common architecture approach in managing and creating its information technology. Part of this process is to treat each technology project as an investment and therefore enhancing the agency's ability to make sound decisions regarding project benefits and priorities as well as resource trade-offs. An enterprise-wide approach to information technology systems ultimately will be more cost-effective since these systems will consistently integrate better with the adoption of more standardized tools wherever and whenever possible. This approach to systems development is core in establishing a robust and effective enterprise-wide security and information management program, which is needed to insure the safety of the agency's and employee information.

The Office of Technology and Information Management (OTIM) spent much of the last year enhancing and improving the reliability of its systems and applications. In addition to a new IT management team a Help Desk function was introduced, the networks were stabilized and bandwidth was more than doubled. An Investment Review Board was instituted to review IT-related expenditures, the software releases of the Risk-Based Capital model were on schedule, the Automated Supervisory Tool – xWorks software was released, and testing of the COOP hot-site was performed. In essence 2006 saw significant shoring up of critical IT functions within the agency - enhancing existing infrastructure.

During 2007 and beyond OTIM will continue to improve the operational infrastructure. OTIM plans to maintain system ownership with the appropriate program office or within OTIM for systems used in multiple offices. Ownership will principally include definition of system requirements which OTIM staff will help elicit and document. OTIM will also develop and disseminate standardized tools for the project management of the applications and will work with the program offices to ensure that appropriate plans are in place for each system to comply with the agency's architectural standards. Additionally, during FY 2007 and FY 2008, Earned Value Management will be instituted for major projects. Furthermore OTIM will assist the other administrative offices in developing the appropriate planning and investment documentation regarding the agency's applications. This will be a significant move for the agency which historically

has not expended significant effort in planning, documenting, and architecting its systems.

At the same time the agency will begin to make certain that it has a robust security program that complies with the applicable regulations and laws including FISMA and the OMB Circular A-130. An important part of this effort will be integrating the security program with the development and deployment process of our systems on an enterprise-wide basis. The agency will also examine the information security practices and systems of other federal agencies as well as private sector organizations to further enhance the security of our information and information systems.

The next five years will be busy and exciting as the agency improves it existing processes and acquires new systems for managing the agency's important mission.

TABLE OF CONTENTS:

INTRODUCTION

The OFHEO Technology and Information Management Five Year Strategic Plan (Plan) is aligned with the agency Director's priorities and the initiatives contained in the agency's Strategic Plan, which sets the course for achieving the overall mission of the agency. Business and technology decisions are made cooperatively to improve the efficiency and effectiveness of the agency programs. The Plan details the office's goals and initiatives for the FY2007 – FY2011 time horizon, presenting a vision for the use of information technology in the agency and a description of how OTIM activities help support the successful accomplishment of the agency's mission, strategic goals and objectives. The Plan is a key component in the capital planning and investment control process that is used for the ongoing selection and evaluation of investments in information technology resources.

Security of information is also addressed in the Plan. A large percentage of the data and documents that the agency creates and receives contain business, confidential or proprietary information, the release of which could cause competitive harm to Fannie Mae and/or Freddie Mac, hereinafter referred to as the Enterprises. Data submitted by the Enterprises provides the basis for the agency's work in capital classification, analysis of risk-based capital requirements, Risk Based Capital Model[1] development, the examination process, and much of the agency research and analysis of the financial markets. In addition, many of our administrative documents and data contain personal information protected by the Privacy Act. An effective security program is of paramount importance in protecting these data and documents as well as the applications in which these data and documents reside.

An important characteristic of the Plan is to ensure that it adequately supports the mission and needs of the agency as well as coordinating with other appropriate federal guidelines. As a consequence the Plan will be reviewed at least semiannually to ensure that it is consistent with the agency's Five Year Strategic Plan and the President's Management Agenda. As part of the review an assessment will be performed to determine if the Plan requires revision to meet any emerging needs of the agency's supervisory, administrative or legal staff. This Plan will be reviewed for consistency with the President's Management Agenda during the first quarter of fiscal year 2008.

I. OFHEO's MISSION AND STRATEGIC GOALS

OFHEO Mission

"To promote housing and a strong national housing finance system by ensuring the safety and soundness of Fannie Mae and Freddie Mac."

[1] The suite of econometric, financial and accounting models used to run the Risk-Based Capital Stress Test and related risk analysis simulations.

The agency's mission statement reflects its congressional mandate to ensure the safety and soundness of the Enterprises and emphasizes the need to foster the strength and vitality of the nation's housing finance system. It also recognizes that success in carrying out this mission promotes a robust housing sector and a strong economy. The agency has established three strategic goals to support the achievement of the agency's mission.

The strategic goals are:

- Agency Strategic Goal #1: "Enhance supervision to ensure the Enterprises operate in a safe and sound manner, are adequately capitalized and comply with legal requirements."
- Agency Strategic Goal #2: "Provide support for statutory reforms to strengthen our regulatory powers."
- Agency Strategic Goal #3: "Continue to support the national policy of an efficient secondary mortgage market which promotes homeownership and affordable housing."

1. Agency's Resource Management Strategy:

"Manage effectively the agency's human capital and other resources to support the agency mission."

The agency's success in achieving its strategic goals depends on the effective management of resources and seamless financial, administrative and information technology support functions. The size of the budget in relation to the mission requires the agency to use limited resources efficiently and ensures that resources are tied directly to the achievement of the mission. As a small but growing agency, the agency relies on staff and management to accomplish its goals through cross-organizational teams that are results-oriented. Agency managers use timely information for decision-making that links strategic planning, program performance, budget, and operational strategies. The agency uses appropriate private sector sourcing and cross sourcing with other government agencies to provide efficient and cost effective services. Additionally, the agency is actively evaluating opportunities for competitive sourcing. The agency's management philosophy drives the efforts to advance the government-wide management goals outlined in the President's Management Agenda.

2. Agency's Information Resource Strategic Goals

OTIM has adopted several strategic goals related to deployment, creation, and acquisition of IT-related technologies. The intent of the goals is to support the overall strategic goals and mission of the agency by ensuring that the supervisory, legal, and administrative functions of the agency have the appropriate technology tools available to effectively achieve these overall goals. Furthermore OTIM seeks to deliver these tools in a cost-effective and coordinated fashion with the appropriate security safeguards to protect the confidential information and systems utilized in conducting OFHEO's business. The strategic goals related to the agency delivering IT-related services include:

- IT Strategic Goal #1: Enhance the efficiency and effectiveness of the agency's Examination, Policy, and Research functions through maintenance, enhancements, and support of key applications including:
    - AST also known as xWorks
    - Risk-Based Capital Stress Test Model [mandated in the Federal Housing Enterprises Financial Safety and Soundness Act of 1992 (Title XIII of P. L. 102-550)] (RBCSim)
    - Supplemental Risk-Based Capital modeling (e.g. Asset-Liability modeling)
    - Agency's Data Repository (e.g. Historical Loan Performance Data)
    - Other systems identified to support the agency's mission

- IT Strategic Goal #2: Enhance the efficiency and effectiveness of the agency operations through the appropriate application of information technology including tools to support the needs of the agency's users.

- IT Strategic Goal #3: Ensure the availability, reliability, scalability, and security of the agency's computing infrastructure and systems.

- IT Strategic Goal #4: Coordinate the development of IT-related systems at the agency by centralizing and standardizing the general planning and security processes to ensure the robustness of these programs.

- IT Strategic Goal #5: Manage IT-related expenditures whenever possible by developing systems using a "best execution" strategy which compares the costs of developing new applications using internal resources, external resources or a combination of both. The best execution strategy will be approved by the Investment Review Board and fit within the approved agency enterprise architecture.

3. Agency's Information Resource Fiscal Year 2007 Major Initiatives

1. Make the security function more robust:
    a. Develop a comprehensive plan for implementing an enterprise-wide security program that addresses the agency IT systems comprehensively and coordinates with the agency's physical security program by end of December 2007.
        i. Conducting internal reviews of the agency's security program to ensure that the program successfully achieves an enterprise-wide orientation.
        ii. Completing the certification and accreditation of all OFHEO systems by September 30, 2007.
        iii. Comply with OMB Memo 06-16. All components have been implemented. Agency policies on data extracts need to be reviewed and updated by 9/30/2007.
    b. Hire additional security staff specialists [completed as of 6/11/2007].
    c. Encrypt all laptop hard drives [completed as of 3/30/2007]

d. Upgrade access to the agency network via two factor authentication or equivalently secure process [completed as of 6/11/2007].

2. Enhance existing staff skill sets to include more subject matter expertise and general problem solving skills.
    a. Maintain the industry best practices of a 50 to 1 ratio of agency staff to Help Desk staff direct support staff / contractors
    b. Recruit software developers with interest or background in pertinent areas of subject-matter expertise (e.g. financial engineering)
    c. Recruit and retain developers to enhance the AST
    d. Recruit an Enterprise Architect to assist in enterprise-wide planning of the IT requirements to provide support of future systems and users at the agency [completed as of 4/15/07].

3. Coordinate the budget process acquisition of IT assets for the Supervisory, Administration and Technology areas:
    a. Focus the Investment Review Board on project based initiatives that support the agency's mission and strategic goals [completed].

4. Infrastructure:
    a. Move mission critical systems to hardware and software that is less susceptible to failure or in the event of a failure of a server the application will automatically switch to a back-up server.
    b. Implement the Metropolitan Ethernet connection as the main source of communication between the home office, 1750 Pennsylvania Ave and the two Enterprises.
    c. Establish and enhance each system's Production, Test and Development environments.

5. Planning Function:
    a. Develop and complete an agency-wide System Development Lifecycle (SDLC) [completed as of 6/21/07].
    b. Work closely with the IRB to ensure that enterprise-wide IT planning and budgeting are coordinated and integrated.

4. Scorecard for Performance Measurement

Each year the agency will review its metrics for measuring the successful achievement of its strategic goals and initiate execution for the upcoming year. Many of these metrics are expected to be persistent – that is to remain in effect each year of the plan with modification of the actual metric level to reflect either the emerging needs of the agency or evolution of processes. New metrics may be introduced to reflect new agency initiatives and goals or to serve as improved measures of existing processes. The measures will be coordinated to reflect the overall strategic plan for the agency as well as the President's Management Agenda. While the metrics will pertain to the collective goals and initiatives, individual metrics may relate to multiple goals and initiatives. A desirable characteristic for the performance metrics is that they form a parsimonious

collection of indicators that can be used and understood by agency's management in assessing performance of its Information Technology-related work.

The key metrics for performance measurement for fiscal year 2007 include:

1. Information Security
    a. Complete the Certification and Accreditation process for all major OFHEO systems that were in production at the end of fiscal year 2006.
    b. Review and provide options to the Director for the reporting structure for OTIM for compliance with FISMA and Clinger-Cohen.
    c. Achieve 80% of the target dates in the Interim Information Security Action Plan (this plan needs to be finalized and has been circulated for review within the Agency).
    d. Develop a comprehensive Information Security Strategic Plan from the Interim Information Security Action Plan including migrating the Agency to an enterprise-wide security program

2. Planning
    a. Develop procedures and guidelines to support the agency's migration to an enterprise-wide development environment (standardization of processes, software, and systems for the agency's applications). The enterprise-wide environment will be the agency's system development life-cycle process (SDLC).
    b. Revise the Investment Review Board's requisition process to be project-based (as opposed to requisition-based) and train the agency's staff in these processes.
    c. Complete the five year strategic plan for the Automated Supervisory Tool.
    d. Develop a preliminary project plan template for agency offices owning applications systems (e.g. the asset-liability management system) and facilitate completion of these plans with those offices.

3. Infrastructure
    a. Complete installation of the Metropolitan Area Network to enhance supervisory productivity and network reliability.
    b. Reassess all systems to identify those that require high-availability and develop recommendation to provide such support.
    c. Provide support for COOP testing and prepare and deploy budgeted COOP hardware and software as identified by the COOP Plan.
    d. Respond to all Help Desk calls within four business hours and complete 85% of all calls within committed close times.

4. Application-Related
    a. Support the Risk-Based Capital classification process in accordance with the time-frames established for OFHEO.
    b. Post implementation reviews of application or system changes.

II. ROLES WITHIN OFHEO

1. Director of OFHEO

The Director of OFHEO has the ultimate responsibility for managing the agency and ensuring that the information policies, principles, standards, guidelines, rules, and regulations are developed and implemented. The Director appoints a Chief Information Officer, who carries out the agency responsibilities listed in the Paperwork Reduction Act, the Clinger Cohen Act, as well as Executive Order 13011.

2. Chief Information Officer

The Chief Information Officer (CIO) develops the OTIM Strategic Plan and defines the Agency's IT vision and strategy. The CIO also insures that IT investments support the agency's mission, strategic goals and objectives. The CIO ensures the application of technology in support of the agency's Strategic Plan, the target IT architecture that effectively supports the agency's activities, IT-related plans for the agency and IT capital planning.

The Chief Information Officer is responsible for:

1. Being an active participant during all agency strategic management activities, including the development, implementation, and maintenance of the agency strategic and operational plans;

2. Advising the Director on:

    a. information resource implications of strategic planning decisions; and,

    b. the design, development, and implementation of information resources;

3. Being an active participant throughout the annual agency budget process and recommend investment priorities for agency information resources through the agency's Investment Review Board (IRB).

4. Recommending internal agency information policies and procedures and oversees, evaluates, and otherwise periodically reviews the agency information resources management activities for conformity with the policies set forth in the IT regulatory statutes;

5. Developing agency policies and procedures that provide for timely acquisition of required information technology;

6. Maintaining an inventory of the agency's major information systems, holdings, and dissemination products , as required by the Paperwork Reduction Act and the Freedom of Information Act (the Records

Management function at the agency is generally responsible for most requirements related to these Acts):

7. Ensure that the agency:

    a. cooperates with other agencies in the use of information technology to improve the productivity, effectiveness, and efficiency of Federal programs;

    b. promotes a coordinated, interoperable, secure, and shared government-wide infrastructure that is provided and supported by a diversity of private sector suppliers;

    c. develops a well-trained staff of information resource professionals

8. Utilize the guidance provided in OMB Circular A-11, "Planning, Budgeting, and Acquisition of Fixed Assets," to promote effective and efficient capital planning within the organization. Ensure that the agency provides budget data pertaining to information resources to OMB, consistent with the requirements of OMB Circular A-11;

The Office of Technology and Information Management is divided into three groups: Technology Management and Development; Customer Service and Operations; and, Information Security:

3. Deputy CIO (Manager of Technology Management and Development)

The Deputy CIO (who serves as the Manager of Technology Management and Development or TMD) is charged with planning and managing related to the day-to-day management of software engineering (application systems development) and technology management. In this capacity the Deputy CIO oversees and coordinates the development activities of all major applications and is charged with developing standardized enterprise-wide procedures related to IT systems development and their security. The centralized planning activity is new to OTIM to ensure that new systems, whether built within the agency or acquired externally, follow consistent and standardized procedures. The agency and the CIO recently separated the CISO functions into a separate position.

4. Manager of Customer Service and Operations Group

The Manager of Customer Service and Operations Group (CSOG) is charged with the day-to-day management of the Customer Support, Systems Engineering and Network Engineering functions. This is inclusive of the day-to-day operation of the IT infrastructure. As such the Manager of CSOG is charged with oversight of the agency's Help Desk and ensuring that IT technology user issues are quickly resolved as well as ensuring that all production systems and infrastructures are: maintained; appropriately backed-up; are available with high-reliability during operating hours; recovered expeditiously in the event of a system or hardware failure, available in the event that a continuity of operation plan must be exercised; properly installed, acquired, and

configured; and, are appropriately monitored and supervised from a security perspective. This management position reports directly to the Chief Information Officer.

5. Chief Information Security Officer (CISO)

OFHEO recently reorganized its information security staff to work directly under the supervision of the CIO. One of the senior staff will be designated to serve as Acting Chief Information Security Officer and will be charged with working with the CIO to develop a comprehensive and robust information security plan. The designated CISO will also provide day-to-day monitoring of the implementation of the agency's security plan and program. The recent organizational change insures better alignment with FISMA.

Appendix A contains the OTIM organization chart.

III. INFORMATION SYSTEM AND RESOURCE REQUIREMENTS

Agency staff must have the tools necessary to carry out their work in an efficient and effective manner. These tools include appropriate technology integrated for effective internal work teams and external communication. To assist in this effort, the agency uses a standards-based, open system environment to increase efficiency and compatibility among systems and to reduce the maintenance burden associated with extensive desktop applications. The agency enhances the integrity and reliability of its information technology infrastructure through automated systems and network management tools.

Information submitted by the Enterprises provides the basis for the agency's work in capital classification, risk-analysis, financial simulation model development, the examination process, and much of the agency research and analysis of the financial markets. The agency will also continue to build its data repository with information on housing and mortgage activity, to provide a repository of aggregated data for research and analysis by the agency. The agency will continue to strengthen the data repository and its surrounding processes that facilitate data sharing, data re-use and interoperability across the agency's information systems.

The agency will continue to manage information technology projects as investments. Projects will focus on identifying and producing measurable process improvements and apply risk management principles.

IV. APPLICATIONS ARCHITECTURE

1. Architecture Objectives

An Applications Architecture is an organization-wide framework, which identifies applications and defines the standards, tools, and components used by applications and communication programs. It describes how the organization's functions are supported through automated information processing. Representing a future vision or extension of the current environment, an Applications Architecture outlines strategies for incorporating the capabilities desired in the current environment but lacking at present. An Applications Architecture governs communication protocols and methods of data

collection and handling. In addition, it should enable system-wide access to data (as security permits) in a common standardized format. Applications Architectures also describe the implementation of reusable objects and services (e.g., class libraries, tools) to support processing that is repeated across applications and Office functions.
The agency applications architecture derives directly from the agency's strategic and performance goals outlined in the Agency Annual Performance Plan. The agency applications architecture has the following objectives:

- Promote agency-wide information sharing.
- Achieve a secure environment and a flexible IT infrastructure that is responsive to change.
- Provide reusability, interconnectivity, scalability, and portability.
- Minimize development, maintenance, and training costs.
- Have a common configuration management process across all IT projects.

Of course, the achievement of the above objectives must be balanced against the need to maintain an appropriate level of security over the information that resides in OFHEO's applications. Much of the information stored and processed by OFHEO's applications is of a proprietary and/or confidential nature, and must be appropriately safeguarded from unauthorized disclosure or modification.

2. Applications Strategy

To achieve the application enterprise architecture objectives, the agency uses the following strategies:

- Perform a cost-benefit analysis to determine if an application should be implemented in-house, outsourced / cross- serviced, or use a Commercial off the Shelf (COTS) package. Each of the alternatives below are analyzed to determine the overall fit within the approved enterprise architecture.
  - Develop a new system in-house if the cost benefit analysis is in favor of in-house development.
  - Use outsourcing or cross-servicing agreements wherever practical to provide services. Given the agency's small size, it is not always economical to implement certain applications in-house. For example, the agency uses cross-servicing agreements to provide payroll systems, and licenses the INTEX CMO model and database to model complex securities as part of the Financial Simulation Model.
  - Leverage COTS products and services. Evaluate outside products and services as part of initial project analysis; use products that work well with the agency's technical architecture; leverage best practices built into COTS to minimize agency-specific customization. For example, the agency uses several COTS packages to implement its Data Strategy.

- Earned Value Management:

- During FY 2007 and FY 2008 OTIM will initiate the use of Earned Value Management as part of the agency project management practices.

- Facilitate agency-wide data sharing – Centralize all Enterprise and housing-related analytic data in the data repository and provide the tools and training to maximize the use of the data. Access to the data is subject to appropriate use guidelines due to the sensitive nature of the data.

- Facilitate agency-wide sharing of supervisory documents by centralizing all Enterprise and housing-related supervisory documents in AST.

- Manage the proliferation of applications – Establish standards for office productivity applications, software development tools, data analysis tools, etc. By using standard tools and applications, development, maintenance and training costs are lowered and the ability to re-use and interoperate is heightened.

Use of these strategies should improve the agency's access to and use of information needed to support day-to-day mission activities associated with ensuring the safety and soundness of the Enterprises. Descriptions of specific agency applications associated with the agency Strategic Goals are contained in the following section.

3. Agency Applications

OTIM plans, develops, secures, maintains, and assures the quality, integrity, confidentiality and availability of the agency's information systems and information assets. This office is responsible for establishing and implementing policies, procedures and standards in the following areas: information systems development and procurement, office automation, information systems security and other information technology-related services.

OTIM's mission statement reflects that IT and information security are critical to the accomplishment of the agency mission. Each office within the agency has a part to play in delivering the products and services associated with the agency mission. There are several office-wide application initiatives that support agency's mission such as:

- Implement and continually improve a data reporting tool that interacts with the agency data repository. This tool will allow the OFHEO divisions to assess the Enterprise data and produce analytical reports.

- Implement and continually improve the AST which provides users a tool to assist users in their supervisory work of the GSEs. AST is a document storage, records management and workflow system that allow users to organize their work papers into Activity Folders that are derived from the approved work plans that management sets out to support the supervisory program.

- General Support Systems are used by all agency employees.

Technical Appendix B describes the function of each office within OFHEO and its major applications.

All of the offices use the General Support Systems. Many of the offices also use specialized software to aide them in performing their functions more efficiently.

4. Investment Review Board and Enterprise Architecture

Commencing at the end of the third quarter of Fiscal Year 2007, the agency will establish and maintain a formal capital planning and investment control process that links mission needs, information, and information technology in an effective and efficient manner. The process will guide the strategic and operational aspects of Information Resource planning and the Enterprise Architecture by integrating the agency's strategic and performance plans with the agency's budget formulation and execution processes. The capital planning and investment control process will include all stages of capital programming, including planning, budgeting, EVM, procurement, management, and assessment.

OFHEO's Investment Review Board (IRB), which is the agency's capital planning and investment control process, has three components: selection, control, and evaluation. The process is iterative, with inputs coming from all of the agency plans and the outputs feeding into the budget and investment control processes. The goal is to link resources to results. The agency's capital planning and investment control process builds from the agency's system requirements and as the agency transitions from its current enterprise architecture to the target enterprise architecture. The new processes will be integrated with the budget process.

During the selection process OTIM creates an analysis of capital expenditures to determine the best execution when implementing a new system or process. OTIM produces three cost estimates which compares the cost and benefit of:

- In-house development
- Implementing a COTS package
- Out sourcing.

The three cost-benefit analyses yields a comprehensive view of the potential solutions, which yields the best execution for the agency. If the agency were to exclusively use one type of analysis or a specific implementation strategy, it could yield a project that may be of less net value to the agency than if the three analyses were compared. This decision making process is paramount for running an efficient organization, as the analysis demonstrates that a projected return on investment is clearly equal or better than the alternatives. This process requires that OTIM to be involved in the initial planning of systems and data requirements.

Once an execution strategy has been chosen for a project, each project will need to compile an EVM analysis. As the project progresses from concept to implementation and

maintenance, each project manager must produce an EVM analysis. Periodically, the updated EVM analysis will be presented to the IRB.

The CIO documents and prepares a revised Enterprise Architecture when significant changes to the existing Enterprise Architecture occur. The revised architecture will be presented to the Director and the IRB prior to allocating funds to implement the changes. An Enterprise Architecture is an explicit description and documentation of the current and desired relationships among business and management processes and information technology. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The Enterprise Architecture also provides a strategy that enables the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes includes the agency's capital planning and investment control processes, agency Enterprise Architecture planning processes, and agency systems life cycle methodologies. The Enterprise Architecture defines the principles and goals and sets the direction on such issues as the promotion of interoperability, open systems, public access, end user satisfaction, and IT security. The agency supports the Enterprise Architecture with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail.

OTIM incorporates security into the architecture of its information and systems which support the agency business operations. Plans to fund and manage security are built into life-cycle budgets for information systems. OTIM has implemented a process which ensures that the security controls for the components, applications, and systems are consistent with and an integral part of the Enterprise Architecture of the agency.

OTIM also identifies additional security controls that are necessary to minimize risk to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control.

OFHEO acquires Information Technology by making use of adequate competition allocating risk between the government, contractor and maximizing the return on investment when acquiring information technology.

V. DATA

1. Architecture

Data is one of the agency's most valuable assets. Information submitted by the Enterprises provides the basis for the agency's mission-related work in capital classification, risk-analysis for risk-based capital, the examination process, and much of the agency's research and analysis of the financial markets. The information is managed in the agency data repository.

The data repository's information will continue to expand to support the agency's mission. Currently, the data repository includes information on:

- Single Family Loans
- Mortgage-Backed Securities
- Loss Mitigation
- Loan Performance
- Multifamily Loans
- Asset-Backed Securities
- Loss Severity
- Credit Enhancements
- Non-Mortgage Financial Instruments
- Financial Statement Data
- Mortgage Insurers
- House Prices

The following sections describe the strategies that are necessary to support the architecture of the agency's databases. They provide a framework for identifying the agency's data needs, data management, and accessibility.

2. Strategy

The agency's Investment Review Board (IRB) is a cross organizational executive body that evaluates Information Resource projects, such as management of the agency's data repository. The IRB makes recommendations about project priorities and resources to the Director.

Data goals include the following:

- Data is an agency resource,
- When systems are developed, the data needs of all of its users should be considered.
- Data will be readily accessible by anyone who is authorized by the system owner to view it.
- Data will be protected from unauthorized access, alteration, or destruction.

Once a new data need is identified, a coordinated and consistent data request will be formulated jointly between the appropriate agency office and OTIM and submitted to the Enterprises or Federal entity. The data sets will be submitted electronically, directly to the agency, alleviating time and technical constraints. Upon receipt, OTIM will validate the accuracy, format, integrity, and consistency of the data and determine if the delivery is acceptable. OTIM will continue to engage the provider until an acceptable delivery is provided and then will make the data and its documentation accessible in the data repository and to the agency user community. OTIM will apply these principles through the implementation of a data coordination, data management, and database and tool management strategy, which are described in the following sections.

3. Coordination

The Data Strategy will be facilitated by ongoing and up-to-date communication. OTIM maintains a catalog of each data request and additional pertinent information concerning its delivery. Prior to releasing data for use within the agency, OTIM will publish detailed documentation that will facilitate data analysis by authorized users. Additionally, the information that is available includes:

- Data Dictionary
- Data Relationship Diagrams
- Validation Statistics about the data

A data education program will be provided for current employees as well as new employees. The orientation process ensures that all authorized users understand what information and resources are available in the agency. Such a program will enable users to reduce the data learning curve and significantly contribute to project work.

4. Management

In consultation with the agency's Supervisory, Administrative and General Counsel Offices, as appropriate, OTIM will recommend policies and procedures to provide:

- Roles and responsibilities for ensuring data maintenance, availability, disposition and optimum computing performance.
- Data administration functions that directly support the data sharing initiative. These functions include:
  - Coordination of data repository development efforts among the OFHEO Offices.
  - OFHEO-wide impact analysis performed for each new development effort.
- Complete documentation of the agency's data.
- Data naming standards that are developed and enforced. Providing consistency among the standard data names enables users to readily identify the content of data sets from different sources.

5. Database and Analytical Tool Management

There have been tremendous advances in technology to provide users with instant access and analysis of large databases. Instant access, instant results, anywhere, anytime -- the expectation has become commonplace. Technology can support the expectation within reason. These technology changes are accompanied by volatility in the marketplace. Many vendors have left or have been forced out of product markets where they once showed promise. In addition to technology and market changes, OFHEO's information needs are growing. More business variables are being used in complex econometric and financial analyses that require a robust hardware and software environment.

As a result, OTIM identifies and procures COTS software that it will maintain through licensing agreements, as agency standards. For example, OTIM has implemented Oracle, Sybase ASP and MS SQL Server and others on an as needed basis as its standard for

relational database management system platforms. These relational database management systems are used for managing the rapidly growing Data Repository. SAS has and is expected to serve as the agency's statistical software package. Hyperion is the OFHEO standard for Web-based on-line analytical processing and will provide users with a user-friendly graphical user interface for query development support. Accompanying a standard set of tools for the agency is the capability to provide in-house training and expert support. OTIM will continue to develop this capability within its staff through rigorous, ongoing vendor product training.

VI. NETWORK AND TECHNOLOGY

1. Technology Architecture

The agency network provides a variety of services to the agency staff including email communications, file and print services, Internet/Intranet access, database services, and a high-performance modeling and research computing environment. The network is composed of several types of resources including the Network Infrastructure, Windows Servers, Unix Servers, and Desktop PC Workstations. Each of these will be briefly discussed below.

2. Network Infrastructure

The agency Network Infrastructure consists of the hardware resources that provide the basic platform for computer interconnections inside and outside of OFHEO. The "Network" consists of routers, switches, firewalls, VPN Concentrators, DNS Servers, and cabling that interconnect all other OFHEO computing resources. The Network provides secure LAN extensions to OFHEO offices located at the Enterprises offices located in Washington, DC (Fannie Mae) and McLean, VA (Freddie Mac.) It also provides a secure connection to our hot-site located in Sterling, VA.

3. Windows Servers

The Windows servers provide many services to the entire agency staff. These include email, shared office folders, and network-based office file storage (Word Documents, Excel Spreadsheets, etc.) The Windows based server infrastructure is currently built upon the Windows 2003 computing platform and uses Windows Active Directory to provide user authentication for most agency computing resources. Critical portions of the Windows server infrastructure are built using clustering technologies and connected to highly available storage systems to provide maximum reliability and information integrity.

4. UNIX Servers

The agency's UNIX servers provide several services to the agency staff, which include a base for the high-capacity databases maintained by OTIM; a high-performance modeling and research-computing environment to calculate the House Price Index and Risk-Based Capital and other financial modeling calculations; a highly reliable high-performance storage system that is shared between the UNIX and Windows systems. The agency

Financial Information Management System (FIMS) is housed on several UNIX servers; this is the primary internal finance and accounting system used by the agency to conduct day-to-day business. The UNIX servers also provide secure resources for exchange of data between the agency and the Enterprises. Additionally, the agency's main financial modeling tools; SAS, MATLAB and Mathematica are housed on these servers.

5. Personal Computers

The personal computers issued by OTIM provide agency staff with "intelligent" access to the various computing resources available to them.

6. Connected Sites

The agency additionally maintains secure interconnections with the USDA National Finance Center in New Orleans, LA; U.S. Treasury FMS system in Hyattsville, MD; the Office of Personnel Management and the Department of Housing and Urban Development in Washington, DC.

7. System Development Lifecycle

The purpose of the System Development Life Cycle (SDLC) is to establish the management, policies, procedures and practices governing the development of a system.

A. Initiation

The initiation of a system (or project) begins when a business need or opportunity is identified by an agency department. A Project Manager is appointed to manage the project. This business need is documented in a Concept Proposal or project Charter. After the Concept Proposal is approved, the System Concept Development Phase begins.

B. Concept Development

Once a business need is approved, the approaches for accomplishing the concept are reviewed for feasibility and appropriateness. The Systems Boundary Document identifies the scope of the system and requires approval from an Office Director, the IRB, and ultimately the Director prior to starting the Planning Phase.

C. Planning

The project charter is expanded to describe how the business will operate when the system is implemented, and to assess how the system will impact employee and customer privacy. To ensure the products and /or services provide the required capability on-time and within budget, project resources, activities, schedules, tools, and reviews are defined. Additionally, security certification and

accreditation activities begin with the identification of system security requirements and the completion of a high level vulnerability assessment.

Beginning in FY 2007 and FY 2008 the planning process will include EVM, which is a process that provides strong benefits for program management and control. EVM provides for the integration of project scope, schedule and cost objectives and establishes a baseline for a baseline plan for performance management during the execution of a project. Furthermore, EVM provides a sound basis for problem identification, corrective actions and management re-planning on as needed basis.

D. Requirements Analysis

Functional user requirements for data, system performance, security, and maintainability requirements for the system are formally defined. All requirements are defined in sufficient detail for systems design to proceed. All requirements need to be measurable and testable and relate to the business need or opportunity identified in the Initiation Phase.

E. Design

The physical characteristics of the system are designed during this phase. The operating environment is established, major subsystems and their inputs and outputs are defined, and processes are allocated to resources. Everything requiring user input or approval must be documented and reviewed by the user. The physical characteristics of the system are specified and a detailed design is prepared. Subsystems identified during design are used to create a detailed structure of the system. Each subsystem is partitioned into one or more design units or modules. Detailed logic specifications are prepared for each software module.

F. Development

The detailed specifications produced during the design phase are translated into hardware, communications, and executable software. Software shall be unit tested, integrated, and retested in a systematic manner. Hardware is assembled and tested.

G. Integration and Test

The various components of the system are integrated and systematically tested. The user tests the system to ensure that the functional requirements, as defined in the functional requirements document, are satisfied by the developed or modified system. Prior to installing and operating the system in a production environment, the system must undergo certification and accreditation activities.

H. Deployment

The system or system modifications are installed and made operational in a production environment. The phase is initiated after the system has been tested and accepted by the user. This phase continues until the system is operating in production in accordance with the defined user requirements.

I. Operations and Maintenance

Once the system operation is ongoing, the system is monitored for continued performance in accordance with user requirements, and needed system modifications are incorporated. The operational system is periodically assessed through in-process reviews during normal operations, which are used to determine how the system can be made more efficient and effective. Operations continue as long as the system can be effectively adapted to respond to an organization's needs. When modifications or changes are identified as necessary, the system may re-enter the planning phase.

J. Disposition

The disposition activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future if necessary. Particular emphasis is given to proper preservation of the data processed by the system, so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies, for potential future access.

This SDLC calls for a series of comprehensive management controls:

- Life cycle management should be used to ensure a structured approach to information systems development and operation.
- Each system project must have an actively involved sponsor.
- A single project manager must be appointed for each system project.
- A comprehensive project management plan is required for each system project.
- Data Management and security must be emphasized throughout the Life Cycle.
- A system project may not proceed until resource availability is assured. The SDLC phases and controls outline a framework which ensures an orderly and comprehensive life cycle development. All agency information resource projects must follow this outline to ensure that each project undergoes the same amount of rigorous overview.

8. Project Management and Planning

During Fiscal Year 2007 OTIM will implement a formal project planning environment that will be modified over time on an as needed basis. The initial project planning documents will consist of templates for project planning and the review of project progress and systems. As noted previously in the document, EVM will be instituted during FY 2007 and FY 2008. Throughout the remainder of FY 2007 additional

documents will be developed to correspond to the development methodology outlined below.

Project management and planning has ten distinct steps identified below.

A. Define the Work: Project Definition

Prior to commencing any project upfront time must be spent for planning to make sure that the work is properly understood and agreed to. This is the time the project manager spends ensuring that the project team and the client have common perceptions of what the project is going to deliver (Business Requirements), when it will be complete, what it will cost (an estimate of the hard and soft costs), who will do the work and how the work will be performed. A key deliverable of defining the work is the Project Definition, which influences the remaining nine steps of the project management and planning process.

B. Build the Work Plan and Budget

The project work plan and budget are created in conjunction with the Project Definition deliverable from the first step. The work plan is a vital tool to ensure that the project team knows what they need to do. Additionally, once the work plan and budget and the EVM analysis is completed, the project team must present this plan to the IRB for review and then forwards to the Director for approval prior to the start of any work.

The approved project budget represents the amount of money available to spend from the agency's appropriated funds and occurs prior to the detailed work plan.

C. Manage the Work Plan and Budget

The work plan and budget are a living document with frequent updates during the life of a project. The work plan and budget represents the current state of the project at a point in time. It is essential that the work plan and budget track how much work remains and how much money is left to complete the remaining work throughout the life of the project.

The work plan describes the timing of the deliverable, the work that needs to occur, the order of the activities, the effort that is required, the assigned resources, and other key aspects of the project. However, the work plan represents the project manager's approximation as to how to complete the remaining work at any particular point in the project.

D. Manage Issues

Issues management is one of the fundamental aspects of the Project Management Process and it is one of the skills that all project managers must feel comfortable dealing with on a proactive and reactive basis. Project management utilizes an issues

log to communicate with the project sponsors and customers. Issues must be resolved quickly and effectively.

E. Manage Scope

Scope is the term used to describe the boundaries of the project and defines what the project will deliver and what it will not deliver. For larger projects, it can include the affected organizations, the transactions impacted, the data types included, etc.

When IT projects fail, it is usually because of one or both of the problems listed below:

- The team did not spend enough time defining the work and/or there was a lack of scope management (i.e. deficiency in requirements gathering)
- The project manager did not manage the project to the agreed-upon scope, so the project scope grew beyond what was originally planned.

The purpose of scope change management protects the viability of the approved Project Definition and the approved business requirements. In other words, the Project Definition defines the overall scope of the project, and the business requirements define the deliverables in detail. The project team must be committed to a deadline and budget based on this high-level and detailed scope definition. If the deliverables change during the project, the estimates for cost, effort and duration may no longer be valid. If the sponsor agrees to include the new work into the project scope, the project manager has the right to expect that the current budget and deadline will be modified (usually increased) to reflect this additional work. This new estimated cost, effort and duration then becomes the approved target after approval by the IRB and the Director.

F. Manage Communications

Properly communicating on a project is critical to success. If sponsors and stakeholders are not kept well informed of the project progress there is a much greater chance that differing expectations of the project will develop. In many cases conflicts arise, not because of an actual problem, but because the sponsor, a stakeholder or the IRB is surprised.

All projects managers communicate the project status on a periodic basis. This includes reporting from the project team to the project manager and reporting from the project manager to the IRB, sponsor and stakeholders. Two typical forums for communicating status are through a status meeting and a status report. Participants in larger projects need to be more sophisticated in how they communicate to various stakeholders. A Communications Plan is the controlling document for how and when status and issues are communicated with the sponsors and stakeholders.

G. Manage Risk

Risk refers to future conditions or circumstances that exist, outside of the control of the project team that could have an adverse impact on the project if they occur. Whereas an issue is a current problem that must be dealt with, a risk is a potential future problem that has not yet, but may occur.

Project managers may employ risk management and risk abatement skills. Problems and risks that can be identified should be managed aggressively through a proactive risk management process.

The project manager will perform a risk assessment with the project team, sponsor and stakeholders. All known risks at the start of the project will be classified as low, medium or high. As the project progresses additional risks may come to light and will need to be reviewed. New and existing risks are communicated through the documents in the Communication Plan.

The purpose of risk management is to identify the risk factors for a project and then establish a risk management plan to minimize the probability that the risk event will harm the project. Additional risk identification should occur throughout the project on a scheduled basis or at the completion of a major milestone.

H. Manage Documents

This step describes the processes and techniques associated with the storing and sharing of electronic and paper documents. The larger a project, the more difficult it is to share information between all the team members and stakeholders. The project manager must have a process designed to manage the documents when the project commences.

I. Manage Quality

Quality management uncovers errors and defects as early in the project as possible. For instance, it is much easier to spot and resolve problems with the business requirements during the analysis phase of the project, rather than redo work to fix problems during testing. The project team should try to maintain high quality and low defects during the deliverable creation processes.

Quality is ultimately defined by the customer and represents how close the project and deliverables come to meeting the customer's requirements and expectations.

A flawlessly designed, defect-free solution that does not meet the client's needs is not considered high quality. The purpose of quality management is to understand the expectations of the customer in terms of quality and then put a plan in place to meet those expectations.

J. Manage Metrics

Managing metrics and managing quality are related. Metrics are used to give an indication of what the beginning state of quality is and whether quality is increasing or decreasing over time. Metrics management can be used effectively on medium and large projects because there is enough time to capture the data, analyze the results and make appropriate changes. Gathering sophisticated metrics on smaller projects will have limited value.

All projects should gather basic metrics information regarding cost, effort, duration and EVM. Metrics can also determine how well the deliverables satisfy the customer's expectations and how well the internal project delivery processes are working.

Project teams should have an approved plan for gathering and utilizing the metrics prior to gathering the raw data to produce the metrics. If the metrics are not used to manage the project there may not be a reason to gather anything other than the basic cost, effort and duration information (unless the metrics are required and utilized at the higher organizational level).

Project metrics are important and most valuable if used to drive improvements on the project and ultimately effecting the overall organization. The accumulation of consistent metrics from all projects can be used to drive process improvements across the organization. Ultimately the information can be used to create a set of best practices and standards that will help all projects.

VII. INFORMATION SECURITY

The agency's security program is an important component of IT resource management. The program is composed of security policies and procedures that are continuously evaluated and modified to effectively protect agency data and other information resources. OTIM is still integrating many of the recommendations from the current and past annual Federal Information Security Management Act (FISMA) audits. Agency systems consist of sensitive but unclassified data comprising large electronic files. The agency has instituted a security program which is based on sound management principles and governing directives. For example, the IT security program is integrated into the system development life cycle from the initiation of the project through development, testing and validation and post-implementation testing. In addition, the agency has implemented policies, controls and safeguards at the agency level to protect the confidentiality, integrity and availability of the data and assets critical to performing the agency's mission.

The OTIM is developing a new enterprise-wide security plan which will consist of the following elements:

- a security architecture common to all applications;
- integration of security into all information system investments; and

- evaluation and integration of new IT security standards and technology into OFHEO's business processes to protect software and hardware from both physical and cyber security threats

The security architecture incorporates the policies, controls and safeguards at OFHEO which protects the confidentiality, integrity and availability of the agency data and its assets critical to performing OFHEO's mission. The systems security architecture will act as a framework for adding new capabilities as well as enhancing or replacing existing capabilities. The goal of this security architecture is to be fully integrated into the agency's Enterprise Architecture and to be consistent with OMB's Federal Enterprise Architecture model.

1. Security Functions and Responsibilities

OFHEO has implemented a security infrastructure to fulfill its security responsibilities. OFHEO's Chief Information Security Officer reports directly to the Chief Information Officer (CIO) and is responsible for establishing agency-wide information security policies and managing the reporting and monitoring processes to ensure compliance. This is accomplished using the security professionals in OTIM.

This infrastructure includes:
1. OFHEO's security program requirements and procedures;
2. Implementation of governing directives for systems security;
3. Administration of the agency access control program;
4. Management of periodic systems review and a comprehensive security compliance and monitoring program;
5. Educational training and awareness programs to management and employees on systems security operational policies, procedures, and requirements;
6. Serving as the operational focal point for day-to-day information system security issues.
7. Insuring compliance with applicable laws, rules and guidance (e.g. FISMA)

The security personnel work with management to ensure that operational and management controls are in place to safeguard OFHEO's assets.

2. Statutory Requirements

The agency will comply with all statutory security related requirements and directives. These directives will be reviewed at least once per year for compliance by the appropriate agency offices (e.g. OGC, OTIM etc.)

- Privacy Act of 1974
- Federal Managers' Financial Integrity Act of 1982
- Office of Management and Budget Circulars A-123, A-127 and A-130
- Clinger-Cohen Act
- Homeland Security Directives

    - Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7)
    - Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12)
- Presidential Decision Directives
    - Enduring Constitutional Government and Continuity of Government Operations (PDD-67)
- FISMA
    - E-Government Act of 2002 Title III Federal Information Security Management Act (FISMA).
    - Federal Information Processing Standard 199 "Standards for Security Categorization of Federal Information and Information Systems"
    - Federal Information Processing Standard 200 "Minimum Security Controls for Federal Information Systems

The agency has implemented a comprehensive information systems security program in effect that undergoes continuous evaluation and modification to effectively protect agency data and other IT resources.

3. System Development Life Cycle (SDLC) as a Security Strategy

An agency-wide SDLC process will apply to all applications and incorporate appropriate system security into the software design and redesign of all major agency systems. Security involvement begins at the initiation of an application and continues through post implementation.

Additionally, a risk assessment is required for all applications at the origination of the process and also before release to production. This is an inherent part of the SDLC. This process ensures that security safeguards are addressed at every stage of the life cycle process. Security personnel involved with developing a specific system are consulted at each stage of systems development. The security personnel ensure that adequate security has been engineered into the current stage of development prior to the next stage of the development life cycle. This process ensures security functions are developed and tested along with all other system functionality. When validation testing is complete, the appropriate manager completes a system release certification. The software moves to an integration testing stage where an additional release certification is completed. It then moves to a training stage, if needed, and then to production implementation. Recertification is performed every 3 years or with any major change to ensure the system's applications and security functions and security controls are still sufficient to meet the intended objectives.

4. Secure Communications & Authentication

OFHEO is evaluating single sign-on and supplemental authentication devices to facilitate current business processes. This effort is critical to OFHEO's missions because of the agency exchange of sensitive information and data.

HSPD-12 single sign-on and supplemental authentication devices are being examined to facilitate OFHEO's varied business processes. Supplemental authentication devices being considered are Smartcards / RSA devices, tokens or a combination. Agency objectives include interoperability with computing platforms, improvements in user account management, improved authentication controls and strengthened security for mobile users. The implementation of these new devices will contribute to making OFHEO HSPD12 compliant by the October 2007 deadline.

While growth of the OFHEO network has benefited the agency's overall mission, new risks from outside attacks become evident as more outside connections are required for the system. The more sensitive web-based enterprise applications are particularly vulnerable if not protected sufficiently. The first line of defense in mitigating these vulnerabilities is access management technology. Firewalls, encryption, VPN, SSL and PKI complement access management to strengthen the environment.

5. Remote Access

OFHEO uses Virtual Private Network (VPN) technology for users to access the OFHEO network remotely. The VPN allows remote users to securely connect to a private network via two factor authentication, while providing optimum security to the OFHEO Network.

6. Certification and Accreditation Program and Systems Security Plans

To comply with the provisions of OMB A-130 and the Federal Information Security Management Act (FISMA), the agency has established Systems Security Plans for all of its systems identified as meeting the definition of a Major Application or General Support System. The systems owners are responsible for developing and maintaining their plans and ensuring that they comply with the specific guidance in National Institute of Standards and Technology (NIST) Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems. The System Security Plans provide an overview of the security requirements of the system and describe how management has provided both adequate and cost-effective safeguards and controls to meet the NIST requirements. For example, General Support Systems and Major Applications are categorized using FIPS 199 and the categories are based upon potential impact of loss, assigned appropriate security controls, tested, certified and accredited prior to implementation and every three years thereafter, or with any major change.

Agency systems security policy includes a certification and accreditation (C&A) process based upon applicable Federal laws, policies, regulations and standards. The agency will formalize its C&A of information technology major systems processes to comply with FISMA and National Institute of Standards & Technology (NIST) requirements. The agency's C&A program is comprised of key activities consistent with NIST.

These activities are:

- Conduct Risk Analysis and Impact Determination (NIST 800-30 and 800-60, formally FIPS 199);
- Complete System Security Plan (NIST 800-18);
- Ensure Adequate Security Controls implemented per Impact level (NIST 800-53);
- Assess the effectiveness of these Security Controls per NIST 800-53A
- Compile Accreditation package (NIST 800-37); and
- Complete certification and accreditation (NIST 800-37).

7. OFHEO Systems Inventory

FISMA (section 305(c)) amends the Paperwork Reduction Act and requires the head of each agency to develop and maintain an inventory of major information systems operated by or under the control of the agency. The agency maintains an inventory of its major information systems and updates the inventory as changes occur. The agency's core business processes are supported by a complex information technology (IT) infrastructure that includes General Support Systems, Major Applications and related Minor Application subsystems that are essential to ensuring that the agency's business processes are able to operate. The agency has installed and implemented many safeguards to protect the confidentiality, integrity, and availability of the agency's systems and data that are critical to its mission. The systems inventory is one of the agency's many safeguards. The agency updates the system inventory continuously to enhance the agency's identification and mitigation of risk to critical operations. Agency management recognizes that without an assessment of the agency's general support systems, major applications and supporting minor application subsystems, it is difficult to ensure that automated information systems are operating with appropriate levels of protection.

8. Operational Controls

Computer security at the agency involves multiple processing platforms, such as but not limited to; Windows and UNIX based servers, firewalls, routers and personal computers. The hardware and software control access to all of the agency's critical and sensitive computer applications. All users accessing the agency's computing platform are subject to agency rules for users and managers of the agency's automated information resources. Each IT system user is required to have a personal User ID and password. In the future, the agency will require the use of HSPD12 compliant devices to access the agency computing environment.

Application programmers use a special second ID tied to their user profile whenever updating applications and their actions are fully audited. Individual user access is controlled further by the use of profiles. Authorized users are granted access based on the principle of "least privilege" only after they have had their requests for access reviewed and approved by both their management and the appropriate security personnel.

The agency implements audit trails for all agency applications which process sensitive data. The use of audit trails provides assurance that the agency is living up to its responsibility to protect information and processes that is critical to the agency. The

Audit Trail System (ATS) is one of the tools that staff can use to monitor agency data entry activities and to ensure that the integrity of agency systems is maintained.

9. Incident Response Team

The agency's Incident Response Team (IRT) are agency employees whose mission is to assist in the protection of the agency's enterprise architecture by anticipating and responding to potential systems threats and vulnerabilities, and acting in an assessment and advisory capacity. Specifically, the IRT protects the agency systems by:

1. Conducting internal intrusion detection services;
2. Conducting risk assessments and issuing vulnerability assessment reports;
3. Implementing safeguards to prevent non-authorized people from gaining access to agency systems;
4. Researching security advisories issued by Federal and private entities; and
5. Responding to incidents by reporting them, evaluating their seriousness, controlling damage, notifying users, and resolving similar future threats.

Annually, OFHEO contracts with an independent auditor to conduct penetration testing to ensure that deployed Intrusion Prevention System remain effective. Other, additional off-the-shelf products are used to identify and protect the OFHEO network against attempts to gain unauthorized access to network resources from within the network itself.

Additionally, the IRT deals with threats to its electronic systems, to assist employees with handling systems incidents, and to share information concerning common vulnerabilities and threats with external entities. The security response team reports to CISO and is tasked with responding to incidents involving computer systems, Internet and Intranet servers and Local Area Network Servers.

VIII. CONTINUITY OF OPERATIONS

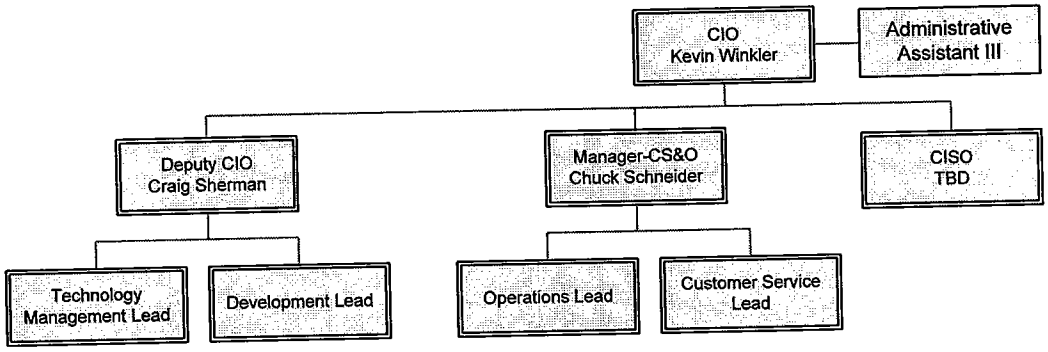
The agency's Continuity of Operations (COOP) plan provides for the resumption of operations in the event of a declared emergency or other unscheduled event that disrupts the agency's normal operations. The plan provides for the restoration of vital records and systems that are critical to the continued operation of the agency and performance of its mission essential activities. OTIM has a comprehensive back-up and recovery process in place that protects of the agency's vital electronic records and systems. This process includes creating backups at OFHEO's main offices and storing the backups at the hot-site and at off-site storage.

During FY2007, the agency will be reviewing and enhancing its COOP plan to ensure the agency has the capability to resume essential operations in the event of an emergency. Each office in the agency will identify and prioritize their vital records and systems for continuity of operations to support essential functions. Essential functions are divided into two categories, mission-related and support-related. Mission-related essential functions include supervisory function, examinations and monitoring capital adequacy. Support-related essential functions include IT support, financial transaction processing, contracting and payroll.

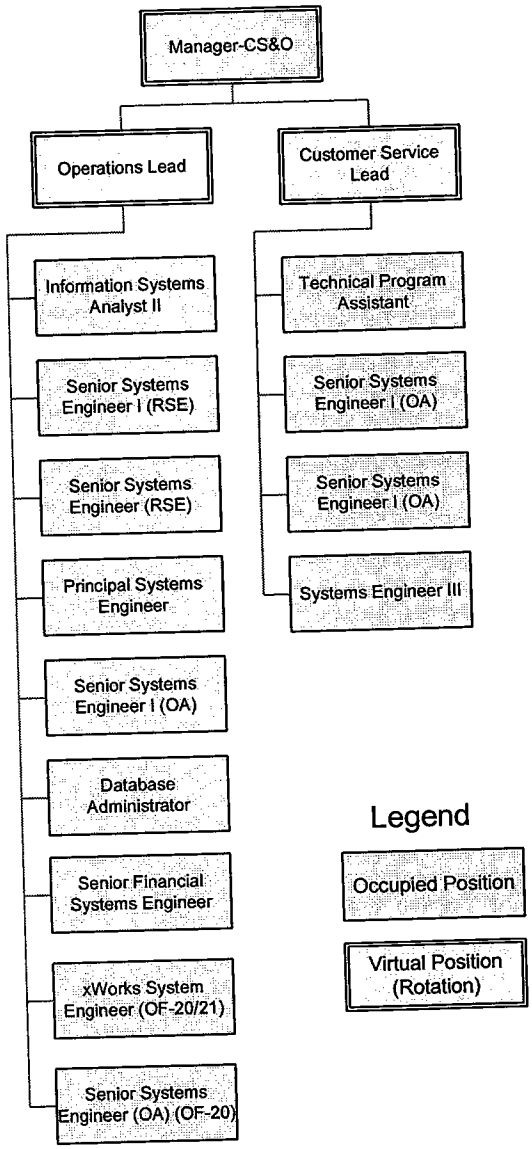
As the agency COOP plan evolves, OTIM will identify and procure the necessary IT equipment and software to support essential functions and a limited number of key personnel at an alternate site, according to the priorities established by the agency's COOP Plan. This will include the hardware, software and communications necessary to establish a secure computer network at the alternate site. In a COOP, this network will be used to maintain continued operations and essential functions for a period of up to thirty days or longer if necessary. As most agency employees will be directed to work from home in the event of a declared emergency, this network will also be used as the primary method of communication between agency management and its employees during the period of the emergency. The COOP Plan will be tested and enhanced in FY2007, according to the guidance provided by Federal Preparedness Circulars, which provides guidance to Federal Executive Branch Agencies for use in developing contingency plans and programs for Continuity of Operations.

Appendix A: OTIM Structure

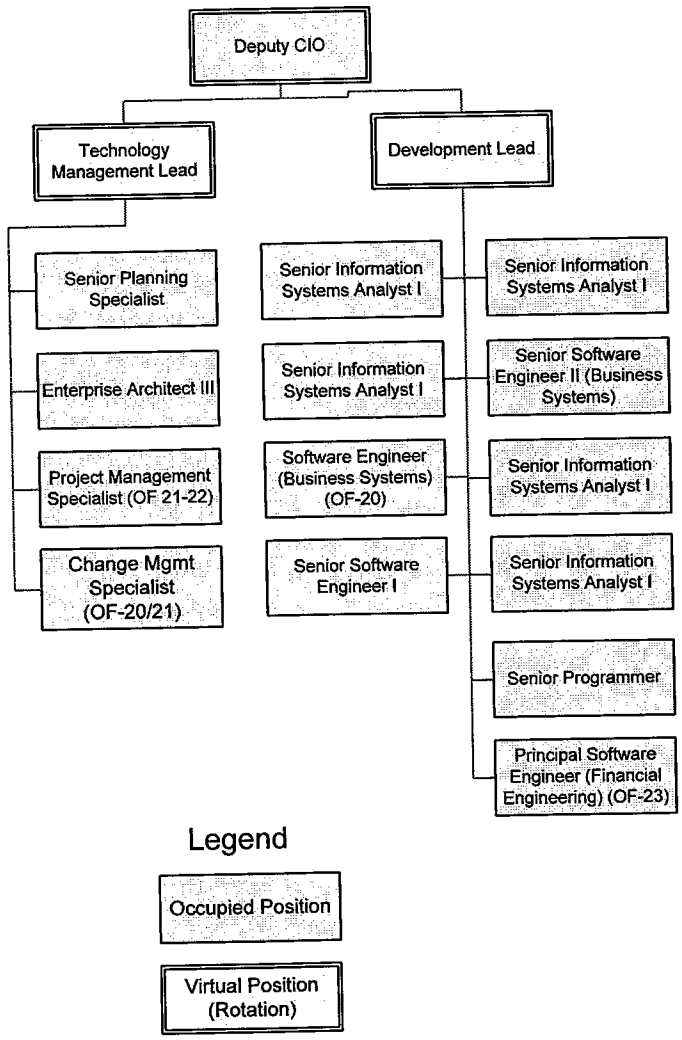
OTIM Organization Chart



Customer Service and Operations Organization Chart



Technology Management and Development Organizational Chart



Appendix B: Description of OFHEO Offices

The **Office of the Director** is responsible for directing and managing the work of all OFHEO offices and staff to meet the agency's mission and goals.

- The Director has exclusive authority under the Act with respect to the management of OFHEO, and is responsible for directing the development, implementation, and review of all OFHEO programs and functions. The Director appoints such personnel as may be necessary to carry out the functions of OFHEO. The Director may delegate to OFHEO officers and employees any of the functions, powers, and duties of the Director, as the Director considers appropriate. The Director may establish and fix the responsibilities of the offices within OFHEO as the Director deems necessary for the efficient functioning of OFHEO.

- The Deputy Director of OFHEO is appointed by the Director in accordance with the Act. In the event of the absence, sickness, death or resignation of the Director, the Deputy Director serves as acting Director until the Director's return or the appointment and confirmation of a successor. The Deputy Director performs such functions, powers and duties as the Director determines are necessary with respect to OFHEO's management and the development and implementation of OFHEO's programs and functions.

The **Office of General Counsel (OGC)** advises the Director and OFHEO staff on all legal matters concerning the functions, activities and operations of OFHEO and of the Enterprises. These matters include, but are not limited to, Enterprise regulatory issues, securities and corporate law principles, administrative law and general legal issues related to operations of Federal agencies. OGC is responsible for interpreting the Federal Housing Enterprises Safety and Soundness Act ("Act") and other applicable laws. OGC brings enforcement actions against the Enterprises and related parties, represents OFHEO in administrative proceedings, and coordinates with the Justice Department and counsel from other agencies as necessary and appropriate. OGC also drafts and coordinates the preparation of legislation and agency regulations

The **Office of Supervision** is responsible for the supervisory program of the agency, and consists of the Office of Examination for both Enterprises, the Office of Chief Accountant, the Office of Compliance, the Office of Capital Supervision, and the Office of Policy and Research. The Director of Supervision is responsible for coordinating smooth operations and for building and enhancing the supervision function of OFHEO, and coordinates with the Office of the Director, Executive Director and Chief and Staff and with the General Counsel.

The **Office of Capital Supervision (OCS)** ensures the comprehensive evaluation and classification of the capital adequacy of the Enterprises, the assessment of risks that impact capital, and the development of tools to measure those risks. This office ensures the integrity of the Enterprises capital classification by effectively managing the production and maintenance of the minimum and risk-based capital (RBC) regulations

and model, and implementing appropriate changes and enhancements to the RBC regulations and model. The office ensures that new Enterprise activities and changes in accounting treatments are assessed timely and thoroughly, and that additional perspectives of risk to capital adequacy are pursued to ensure the agency's assessment of the Enterprise's capital is comprehensive. The Office of Capital Supervision supports the capital adequacy and safety and soundness responsibilities of the agency by researching topics and developing alternative models and measurements of risk and capital adequacy.

- OCS develops and applies econometric, financial and accounting models to evaluate the credit and market risks of the Enterprises, and undertakes other related research and analyses. OCS has developed and continues to maintain and enhance the set of models used for financial simulations of the Enterprises.

The **Office of Compliance (OC)** promotes the safety and soundness of the Enterprises by supervising compliance with statutory, regulatory and agency requirements and ensuring that the agency is informed of emerging issues. OC plans and conducts special examinations of the Enterprises on particular issues or specific areas requested by the Director that are outside the scope of the regular safety and soundness examination process. This office is responsible for identifying and investigating emerging issues and potential weaknesses of the Enterprises and recommending corrective, preventive and enforcement actions, as appropriate.

- OC uses the Litigation Support System, which is a document management system which aids in conducting the special examination of Fannie Mae.

The **Office of the Chief Accountant (OCA)** develops policy on safety and soundness issues related to accounting and financial reporting and monitors all accounting policy related to the Enterprises, working with the enterprises at a policy level as emerging issues arise. This Office provides oversight of the accounting and financial standards functions at the Enterprises. OCA supports other OFHEO Offices to ensure that accounting policy interpretation and implementation are consistent across offices and with the mission of OFHEO. OCA also interfaces with external constituents on accounting issues.

- OCA is the subscriber of the Accounting Research Manager, which aids in performing research on the Enterprise's accounting treatments.

The **Office of Examination (OE)** plans and conducts examinations of the Enterprises, as required by the Act, prepares and issues reports of examination summarizing the financial condition and management practices of each Enterprise, and seeks preventive and corrective actions as appropriate. The office complements its on-site examination activities with off-site financial safety and soundness monitoring.

To reduce OE's dependency on the Enterprises supplying data extracts for analysis, OE should be able to directly access the Enterprise Data and produce analytical reports to deepen agency understanding of the operational risks, credit risks, and interest rate risks that face the Enterprises. In order for OE to optimize their analytical capabilities and

make their recommendations, applications such as AST integrates the risk assessment process, which includes information retrieval and analysis as well as a document and workflow management system.

- OE is the AST system owner and is available to all Supervisory staff and integrates the risk assessment process, including information retrieval and analysis as well as a document and workflow management system.

The **Office of Policy Analysis and Research (OPAR)** is headed by the Chief Economist. OPAR conducts research and policy analysis to assess the short- and long-term impact on the regulatory and supervisory functions of the agency on trends and issues in the activities of the Enterprises, housing finance, and financial regulation. The office also prepares data series, reports, and research papers; and works with other agency offices to develop policy options; and makes recommendations to the Director on a broad range of policy issues.

- OPAR uses data from the agency data repository to develop the agency quarterly publication, the OFHEO House Price Index (HPI), and to make policy recommendations. In order for OPAR to do this, data from other Federal agencies and from commercial sources will be required to be captured, standardized, and stored in the data repository.

- OPAR uses the following software programs to aide in their research and analysis
  - SAS to create the OFHEO Housing Price Index.
  - MATLAB
  - Mathematica

The **Office of Risk Assessment and Financial Performance (ORAFP)** is responsible for performing comparative financial assessment of the Enterprises as well as assessing financial risk assessment of these institutions. This group also provides support in financial analysis for the agency's examination offices. Since this group was just created it information technology needs are not yet fully defined. This group will be active participants in the Call Report system and require access and tools to evaluate the Enterprises financial and other data.

The **Office of Supervision Policy, Systems, and Quality Assurance (OSPSQA)** is responsible for developing and documenting policies and procedures related to the supervision process. This office supports all of the supervision offices by developing standardized workflow processes. This office also serves as the systems owner of xWorks which the system the agency's uses to store examination information and manage the examination process. Since this group was only recently created its information technology needs are still being defined. OTIM supports OSPSQA in the development and deployment of the xWorks system.

The **Office of External Relations (OER)** is headed by the Associate Director for External Relations and includes the Congressional Affairs and Public Affairs functions. The Public Affairs Officer serves as spokesperson for OFHEO.

- OER coordinates contacts with external parties (i.e. the public, media, Congress, trade associations, other regulators, etc.)
- OER utilizes OFHEO's web site to disseminate information to OFHEO stakeholders and the public.

The **Office of Executive Director** is responsible for agency-wide management and oversight of all administrative matters, and consists of the Office of Budget and Financial Management, the Office of Human Resources Management, the Office of Technology and Information Management, and the Office of Strategic Planning and Management. The Executive Director and Chief of Staff is the chief administrative officer of OFHEO, serves as a legal advisor on administrative matters, and coordinates communication and cooperation on administrative issues with the Office of General Counsel.

The Office of the Executive Director:

- Provides executive oversight of the agency's administrative and organizational management, including financial management and budgeting, facilities, property and security management, human resources, diversity and equal employment opportunity management, strategic planning, records and information management, information technology management and compliance with statutory, regulatory and administrative requirements.
- Provides policy advice to Deputy Director and Director on topics related to the agency's infrastructure and administrative functions.
- Coordinates and leads the activities of the four infrastructure offices: Office of Budget and Financial Management, Office of Human Resources Management, Office of Strategic Planning and Management and Office of Technology and Information Management.
- Manages the agency's records management program, which includes coordinating with the Office of the General Counsel all responses to the Freedom of Information Act (FOIA) and Privacy Act requests.
- Manages and oversees the agency's Equal Employment Opportunity programs in coordination with the Office of General Counsel and the Office of Human Resource Management.
- Manages and oversees the agency's privacy program in coordination with the Office of General Counsel.

The **Office of Budget and Financial Management (OBFM)** is headed by the Chief Financial Officer. OBFM provides support services in all areas of financial and administrative management of OFHEO. OBFM is responsible for developing, managing and implementing agency policies and procedures governing:

- Support for all facility and supply requirements.
- Agency contracting and procurement programs.
- Agency financial management, budgeting and accounting functions, including travel, internal controls, and financial reporting.

In order for OBFM to comply with the Joint Financial Management Improvement Program (JFMIP) standards for financial systems and systems that contain financial

information required in the core accounting system, an integrated financial system (FIMS) is used for accounting.

The **Office of Human Resources Management** (OHRM), which is headed by the Chief Human Capital Officer. OHRM provides support services in all areas of human resources, payroll and personnel security of the agency. This office is responsible for developing, managing and implementing agency policies and procedures governing:

- All human resources functions (staffing, employee relations, performance management, training, benefits management, compensation);
- Payroll and processing functions, and
- Personnel security functions.
- Human Resources use AVUE for recruiting and position management.

The **Office of Strategic Planning and Management** (OSPM) assists the Director in developing and maintaining a long term strategic plan that is consistent with the mission of OFHEO and facilitates efforts to ensure that the activities and operations of the agency are consistent with the strategic plan. This office also provides leadership in planning, managing and assessing OFHEO's performance, including the development of OFHEO's annual performance plans and reports. OSPM is also the system owner and responsible for the Agency's Time Study application.

Appendix C: PLANNING AND MANAGEMENT PROCESSES

1. Laws and Regulatory Guidance

A. Clinger-Cohen Act (CCA) of 1996

Section 5125(d) of the Clinger-Cohen Act (CCA) defines information technology architecture as an integrated framework for evolving or maintaining existing IT technology and acquiring new IT technology to achieve the agency's strategic and information resources management goals. A complete IT architecture consists of both logical and technical components.

- The logical architecture provides the high-level description of the agency's mission, functional requirements, information requirements, system components, and information flows among the components.
- The technical architecture defines the specific IT standards and rules that will be used to implement the logical architecture.

The OTIM Strategic Plan addresses the requirements of the Clinger-Cohen Act on Information Technology (IT) planning and management requirements. It also addresses the requirements of managing Federal information resources as expressed in the Office of Management and Budget (OMB) Circular A-130, and the Paperwork Reduction Acts of 1980 and 1995.

CCA requires that agency information technology management be operated as an efficient and profitable business would be operated. Acquisition, planning and management of technology must be treated as a "capital investment." The CIO leads the effort in implementing this statute. CCA covers three governmental activities; providing services, collecting information, and soliciting stakeholder comment. These activities have evolved to online governance and dissemination of information.

CCA emphasizes an integrated technology framework to ensure IT efficiencies. OTIM cannot operate efficiently with hardware and software systems acquired on an "impulse purchase" basis and installed without an overall plan. All facets of capital planning must be taken into consideration just as they would be in private industry, which include:

- cost-benefit ratio
- expected life of the technology
- flexibility and possibilities for multiple uses

B. Paperwork Reduction Act

The Paperwork Reduction Act establishes a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the Act requires that the Director of OMB develop and implement uniform

and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

C. OMB Circular A-130: Management of Federal Information Resources

OMB Circular Number A-130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35. This Memorandum contains updated guidance in Appendix III, "Security of Federal Automated Information Systems," which makes minor technical revisions to the Circular to reflect the Paperwork Reduction Act of 1995 (P.L. 104-13).

D. OMB Circular A-11

Circular A-11 provides guidance on capital planning and other planning processes.

Appendix D: Glossary of Terms:

ATS – Audit Trail System (formerly known as xWorks)
CIO – Chief Information Officer
CISO – Chief Information Security Officer
COTS – Commercial Off the Shelf Software
CSOG – Customers Service and Operations Group
Enterprises – Fannie Mae and Freddie Mac
FISMA – Federal Information Security Management Act
GSE – Government Sponsored Enterprise
GSS – General Support System
HSPD – Homeland Security Presidential Directive
IRB – OFHEO Investment Review Board
IRT – Incident Response Team
IT – Information Technology
OFHEO – Office of Federal Housing Enterprise Oversight
OMB – Office of Management and Budget
OTIM – Office of Technology and Information Management
Plan – OFHEO 5-Year Information Technology Strategic Plan
PMA – President's Management Agenda
SDLC – System Development Life Cycle
TMD – Technology Management and Development
VPN – Virtual Private Network