


**Office of Inspector General**  
**U.S. House of Representatives**  
Washington, DC 20515-9990

**MEMORANDUM**

TO: Jeff Trandahl  
Clerk of the House

FROM:   
Robert B. Frey III  
Deputy Inspector General

DATE: May 17, 1999

SUBJECT: Management Advisory Report - Legislative Information Systems Evaluation  
(Report No. 99-CLK-02)

This is our final report on Legislative Information Systems Evaluation. The objective of this evaluation was to analyze the system alternatives for replacing the Clerk's Financial Disclosure and Lobby Disclosure Act applications. In this report, we discussed areas where safeguards could be implemented to mitigate the risk to the current applications. We also discussed a number of information technology solutions that could replace the current Financial Disclosure and Lobby Disclosure Act applications. Accordingly, we recommended actions with respect to the maintenance and replacement of these current applications.

In response to our February 9, 1999 draft report, your office generally agreed with our findings and recommended actions. The March 1, 1999 management response is incorporated in this final report and included in its entirety as an appendix. The corrective actions taken and planned by your office are appropriate and, when fully implemented, should adequately respond to the recommended actions.

We appreciate the courtesy and cooperation extended to us by your staff. If you have any questions or require additional information regarding this report, please call me or Christian Hendricks at (202) 226-1250.

cc: Speaker of the House  
Majority Leader of the House  
Minority Leader of the House  
Chairman, Committee on House Administration  
Ranking Minority Member, Committee on House Administration  
Members, Committee on House Administration

**TABLE OF CONTENTS**

I.	INTRODUCTION.....	1
	Background.....	1
	Objective, Scope, And Methodology.....	2
II.	RESULTS OF STUDY.....	3
	Needs Statement.....	3
	Risk Assessment.....	4
	Feasibility Study.....	7
	Cost-Benefit Analysis.....	8
III.	RECOMMENDED ACTIONS.....	12
	Immediate.....	12
	System Planning, Development, and Implementation.....	13
	Management Response.....	14
	Office of Inspector General Comments.....	15
IV.	EXHIBITS	
	Exhibit 1: Application Overviews	
	Exhibit 2: Needs Statement	
	Exhibit 3: Risk Assessment	
	Exhibit 4: Feasibility Study	
	Exhibit 5: Cost-Benefit Analysis	
V.	APPENDIX	
	Clerk's Management Response to The Draft Report	



# LEGISLATIVE INFORMATION SYSTEMS EVALUATION

## I. INTRODUCTION

This report presents the results of the evaluation of the system options for replacing the Financial Disclosure (FD) and Lobby Disclosure Act (LDA) applications in the Office of the Clerk (Clerk) with electronic filing, document imaging, data encryption, and/or electronic signature technologies. The report includes the following: (1) a needs statement that presents the high-level business needs for a replacement system, (2) an assessment of the system risks associated with the FD and LDA applications, (3) a feasibility study of viable options for replacing the systems, (4) a cost-benefit analysis of implementing viable options to replace the FD and LDA applications, and (5) a recommended course of action for utilizing the results of the evaluation.

The evaluation was conducted by the Office of Inspector General (OIG) utilizing the services of PricewaterhouseCoopers (PwC). The Clerk's Office assisted the OIG by providing information to facilitate the completion and validate the results of the evaluation.

### Background

The Clerk tracks documents submitted to the U.S. House of Representatives (House) under the Ethics in Government Act (EIGA) and LDA. For the EIGA, Representatives and Delegates of the House, House Officers, certain employees, and candidates running for election to the House must file financial disclosure statements with the Clerk. Disclosure statements are tracked and made available to the public using the FD application. The LDA requires lobbyists to register and provide semi-annual lobbying reports to the Clerk. The registrations and reports are required to be common between the House and the U.S. Senate (meaning the rules, regulations, forms, and collection periods must match). The Clerk tracks and makes these reports publicly available using the LDA application. In both cases, the Clerk is charged with a legal responsibility for public disclosure of all reports filed under the respective acts.

The FD and LDA applications utilize a document capture system called FileNet to capture and index paper generated source data. FileNet is a commercially available software application operated and maintained by the Clerk. The system uses an Oracle database management system, UNIX operating system, and RS-6000 hardware<sup>1</sup>. Documents are scanned into FileNet using Kodak Imagelink and Bell & Howell scanners that allow the images to be stored on optical disk. The documents are indexed on the House mainframe and captured by FileNet using a workflow program. The general public can view the documents by entering query criteria via a FileNet screen at the public workstations in the Legislative Resource Center. Neither of these applications supports electronic filing of documents, data encryption, or electronic signature.

---

<sup>1</sup> UNIX is a common operating system used in computing and RS-6000 is a common mid-range server hardware component.

The Clerk desires to replace both the FD and LDA applications with modern hardware and software that allow for electronic filing, document imaging, data encryption, and electronic signature functionality. In addition, the Clerk desires to implement a solution that can be maintained and operated solely by Clerk resources.

The detailed overview of the FD and LDA applications can be found in Exhibit 1, *Applications Overviews*.

### **Objective, Scope, And Methodology**

The objective of the evaluation was to analyze the system alternatives for replacing the Clerk's FD and LDA applications. The system alternatives focused on the functional and technical feasibility, costs-benefits, and risks of utilizing electronic filing, document imaging, data encryption, and electronic signature technologies to meet the needs and deficiencies of the existing FD and LDA applications. The evaluation of the FD and LDA applications included the performance of the tasks listed below. These tasks were completed in accordance with the House's System Development Life Cycle (SDLC) dated June 28, 1996, which implements procedures detailed in the U.S. Department of Commerce, National Bureau of Standards, Special Publication 500-153, *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach*. Our evaluation approach was to do the following:

- **Gain Understanding of Applications.** Data was collected to gain an understanding of the legislation that the applications support, the functionality, business processes, and the organizations that use and support the applications. The detailed methodology and results of this task can be found in Exhibit 1, *Application Overviews*.
- **Prepare a Needs Statement.** Data was collected to identify deficiencies in existing application capabilities, new or changed program needs, and overall high-level business needs of the two applications as they relate to the Clerk's mission. The detailed methodology and results of this task can be found in Exhibit 2, *Needs Statement*.
- **Conduct a Risk Assessment.** Data was collected to identify the threats to data and assets, the potential impact of those threats, system vulnerabilities, and existing safeguards of the current internal control and security environment of the applications. The detailed methodology and results of this task can be found in Exhibit 3, *Risk Assessment*.
- **Prepare a Feasibility Study.** Based on the analysis of the data collected in the needs statement and risk assessment tasks, a feasibility study was performed. The feasibility study included analyzing the needs, defining evaluation criteria, identifying a range of potential alternatives, and selecting and developing system alternatives. The detailed methodology and results of this task can be found in Exhibit 4, *Feasibility Study*.
- **Conduct a Cost-Benefit Analysis.** The scope of this evaluation included a cost-benefit analysis of the system alternatives identified in the feasibility study. The detailed methodology and results of this task can be found in Exhibit 5, *Cost-Benefit Analysis*.

The work completed in the evaluation of the Clerk's applications was based on the following overall assumptions and constraints:

- **Scalability.** Any potential alternative must be scalable to meet all needs. The scope of this evaluation was the FD and LDA applications, but any potential system alternative must be able to be scaled to meet the needs of other applications within the Clerk's domain or other areas of the House.
- **Use of Commercial-off-the-Shelf Applications.** The House's Information Systems Program Plan, Management Policy for SDLC, states the desire to move towards commercial-off-the-shelf (COTS) applications. For this evaluation, commercially available software was considered for use as the infrastructure for the replacement system. However, in order to meet the unique needs of the Clerk's Office, some customization may be required.
- **Implementation Time Frame.** Plans are currently underway to allow for a migration of all mission critical applications from the House's mainframe operated by the House Information Resources' (HIR) by the third quarter of Calendar Year (CY) 1999. Any potential alternative to replace the current FD and LDA applications should consider that migration plan when planning for the procurement or the implementation process.
- **Economies of Scale.** The alternatives should allow for economies of scale, such as implementing technology that supports both the FD and LDA applications.
- **No Significant Changes to Existing Laws.** The alternatives should not require significant changes to the EIGA or LDA.

The evaluation was conducted during the period July 1998 through November 1998.

## **II. RESULTS OF STUDY**

In this section, the results of the Legislative Information Systems evaluation are presented. The summary includes: (1) a needs statement that presents the high-level business needs for a replacement system, (2) a risk assessment associated with the FD and LDA applications, (3) a feasibility study of viable options for replacing the applications, and (4) a cost-benefit analysis for implementing viable options to replace the FD and LDA applications. Lastly, recommendations for utilizing the results of this evaluation are also presented.

### **Needs Statement**

The purpose of the needs statement was to identify the high-level deficiencies in existing capabilities, new or changed program needs, and overall high-level business needs of the two applications as they relate to the Clerk's mission. The needs statement also identifies opportunities for increased economy and efficiency and provides justification for exploring alternative solutions.

The needs statement was developed based on the analysis of data collected from staff of the Clerk. The results of the needs statement included:

- **Deficiencies.** Deficiencies were identified across both applications as a whole and each individual application. These deficiencies can be summarized as substantial manual data entry, general dissatisfaction with the current FileNet system (i.e., increasing costs to maintain and enhance the current system, as well as the level of vendor support provided), lack of automated interfaces, no automated tracking capabilities, and manual reconciliation.
- **Program Needs.** The system should be flexible enough to allow efficient response to changes in system needs or general duties of the Clerk, without considerable rework of the system and associated business processes.
- **High-Level Business Needs.** The system should provide for the capabilities identified in Figure 1: High-Level Business Needs. The functionality is divided into categories, with a corresponding description of each category.

Category	Description
Input	<ul style="list-style-type: none"> <li>• Ability to minimize the amount of manual data entry during forms processing and database compilation.</li> </ul>
Processing	<ul style="list-style-type: none"> <li>• Ability to allow for the automation of processing tasks (i.e., reporting non-responses and image destruction).</li> </ul>
Output	<ul style="list-style-type: none"> <li>• Ability to provide flexible printing capabilities.</li> </ul>
Query	<ul style="list-style-type: none"> <li>• Ability to provide for flexible record query and reporting capabilities for both public and administrative use.</li> </ul>
Storage	<ul style="list-style-type: none"> <li>• Ability to store images in commonly used and available media.</li> </ul>
Technology	<ul style="list-style-type: none"> <li>• Ability to allow for document imaging, electronic filing and/or signature capabilities via the Internet, as well as provide a network centric platform (client-server) that can be maintained within the confines of the Clerk.</li> </ul>
Application Controls and Security	<ul style="list-style-type: none"> <li>• Ability to authenticate users of the system, to protect data during electronic filing, to provide restricted access to data within the system, and provide for system availability on a timely and consistent basis.</li> </ul>
Data Integrity Control	<ul style="list-style-type: none"> <li>• Ability to provide integrity and control, as noted in the risk assessment.</li> </ul>

*Figure 1: High-Level Business Needs*

The detailed methodology and results of this task can be found in Exhibit 2, *Needs Statement*.

### **Risk Assessment**

The purpose of the risk assessment was to identify threats to data and assets, the potential impact of those threats, system impacts and vulnerabilities to the FD and LDA applications, and recommend safeguards to mitigate the potential threats. Using an internal control and security

diagnostic tool, we gained an understanding of the current vulnerabilities and related safeguards. Information for the diagnostic tool was gathered through observations made during walkthroughs of the systems and facilities, and from interviews with staff of the Clerk and HIR.

The results of the risk assessment indicated that nine high-level threats were pertinent to the FD and LDA applications where the associated data may be vulnerable. These threats originate from events or people internal or external to the House. Figure 2: Summary of Risk Assessment Results on the following page presents these nine threats, the potential impacts and vulnerabilities, and recommended safeguards to minimize or eliminate the threats.

The detailed methodology and results of this task can be found in Exhibit 3, *Risk Assessment*.



<b>Threat</b>	<b>Vulnerabilities</b>	<b>Recommended Safeguards</b>
Acts of nature	<ul style="list-style-type: none"> <li>No business continuity plan (BCP) within the Clerk.</li> </ul>	<ul style="list-style-type: none"> <li>Develop, test, and implement a BCP and document image backup procedures.</li> <li>Use an off-site storage facility consistent with the practices of HIR, to store and maintain tape and/or image backups.</li> </ul>
Acts of terrorism	<ul style="list-style-type: none"> <li>No BCP within the Clerk.</li> <li>Weak physical access controls for Legislative Computer Systems (LCS) data center.</li> </ul>	<ul style="list-style-type: none"> <li>Develop, test, and implement a BCP and document image backup procedures.</li> <li>Use an off-site storage facility consistent with the practices of HIR, to store and maintain tape and/or image backups.</li> <li>Strengthen physical access controls (e.g., implement card key, guest sign-in and double-door access).</li> </ul>
Data center environmental compromise (facilities)	<ul style="list-style-type: none"> <li>No BCP within the Clerk.</li> </ul>	<ul style="list-style-type: none"> <li>Develop, test, and implement a BCP and document image backup procedures.</li> <li>Use an off-site storage facility consistent with the practices of HIR, to store and maintain tape and/or image backups.</li> </ul>
Hardware failure	<ul style="list-style-type: none"> <li>No BCP within the Clerk.</li> </ul>	<ul style="list-style-type: none"> <li>Develop, test, and implement a BCP and document image backup procedures.</li> <li>Use an off-site storage facility consistent with the practices of HIR, to store and maintain tape and/or image backups.</li> </ul>
Intentional acts by House staff	<ul style="list-style-type: none"> <li>Lack of application and system software change control.</li> <li>Lack of integrated security administration.</li> <li>No quality controls present.</li> </ul>	<ul style="list-style-type: none"> <li>Grant access to users based upon job duties.</li> <li>Provide for segregation of duties through workflow functionality.</li> <li>Improve application change control procedures using change control tools.</li> <li>Appoint a security officer to monitor and manage security.</li> </ul>
Fraudulent filings	<ul style="list-style-type: none"> <li>No validation procedures in effect.</li> </ul>	<ul style="list-style-type: none"> <li>No improvements recommended. Inherent safeguard is present. The filer who has been impersonated would likely detect fraud.</li> </ul>
Misrepresentation of identity of public users	<ul style="list-style-type: none"> <li>No manual or automated authentication of application users.</li> </ul>	<ul style="list-style-type: none"> <li>Implement manual or automated authentication procedures that are consistent with the spirit of the EIGA and LDA laws. Example includes increased staff intervention with users that reduce the chance of misrepresentation of the identity of public users.</li> </ul>
Human error by staff	<ul style="list-style-type: none"> <li>Lack of application and system software change controls.</li> <li>No segregation of incompatible duties.</li> <li>Application edits and validations need improvement.</li> <li>The FD and LDA applications do not have strong query capabilities.</li> </ul>	<ul style="list-style-type: none"> <li>Grant access to users based upon job duties.</li> <li>Provide for segregation of duties through workflow functionality.</li> <li>Improve application change control procedures using change control tools.</li> <li>Reduce redundant data entry.</li> <li>Provide for strong application edits and validations.</li> <li>Implement stronger and more precise query capabilities.</li> </ul>
Logical/physical penetration to data center by unauthorized public users	<ul style="list-style-type: none"> <li>Lack of integrated security administration; weak physical access security to data center.</li> </ul>	<ul style="list-style-type: none"> <li>Appoint a security officer to monitor and manage security.</li> </ul>

*Figure 2: Summary of Risk Assessment Results*

## **Feasibility Study**

The purpose of the feasibility study was to identify viable alternatives to the existing system. The feasibility study was intended to provide management with adequate information to make decisions to analyze and evaluate alternative systems to satisfy mission needs.

The results of the feasibility study indicated that four specific alternatives would serve as implementation scenarios for further evaluation. The rationale used to group the viable alternatives was to provide the Clerk with a range of viable alternatives to consider, and analysis of viable technologies. The four alternatives selected for further evaluation in Exhibit 4, *Feasibility Study* include the following:

**Alternative 1: Imaging/Workflow System.** Implement a new, client-server based imaging system that includes advanced forms processing functionality with optical character recognition (OCR)/intelligent character recognition (ICR), and workflow capabilities<sup>2</sup>. This alternative meets most of the evaluation criteria, with the exception of electronic filing. This alternative could be implemented so that it is scalable for future implementation of electronic filing. Primary implementation issues include increased responsibility for the Clerk to manage and maintain a new system, and changes to business processes as a result of the implementation of OCR/ICR and workflow technologies.

**Alternative 2: Imaging/Workflow System and Electronic Filing with Basic Encryption.** Implement a new imaging/workflow system, and add functionality that would allow browser-based submission of FD and LDA forms via the Internet. The system would incorporate Secure Socket Layer (SSL) and Challenge Response security/authentication measures. This alternative meets the evaluation criteria. Primary implementation issues include: (1) increased responsibility for the Clerk to manage and maintain a new system; (2) changes to business process as a result of the implementation of OCR/ICR and workflow technologies; and (3) the use of electronic filing without the ability to guarantee non-repudiation<sup>3</sup>.

**Alternative 3: Imaging/Workflow System and Electronic Filing with an Outsourced<sup>4</sup> Public Key Infrastructure.** Implement a new imaging system, with added functionality that allows for browser based submission of LDA and FD forms via the Internet. The system would incorporate the use of Public Key Infrastructure (PKI)<sup>5</sup> administered by an outsourcing provider. This alternative meets the evaluation criteria and provides additional assurances for non-repudiation.

---

<sup>2</sup> OCR/ICR and workflow capabilities allow for improvements to the core document imaging functionality through optical character features and controlled flow of documents through the system.

<sup>3</sup> Non-repudiation refers to the ability to validate whether a filer actually signed or sent a document to the Clerk.

<sup>4</sup> For purposes of this study, outsourcing refers to administration of a system outside the confines of the Office of the Clerk. This could include outsourcing services provided by an external vendor or another House office (i.e., HIR).

<sup>5</sup> Public Key Infrastructure provides increased levels of confidentiality, integrity, and authentication of electronic submissions.

Primary implementation issues include: (1) limited management control over the issuance of digital certificates; (2) changes to business processes as a result of the implementation of OCR/ICR and workflow technologies; and (3) the appropriateness of implementing a PKI infrastructure specifically for the FD and LDA applications while a need for a House-wide PKI infrastructure may exist in the future.

**Alternative 4: Imaging/Workflow System and Electronic Filing with an In-house Public Key Infrastructure.** Implement a new imaging system, with added functionality that allows for browser based submission of FD and LDA forms via the Internet. The system would incorporate the use of PKI administered by the Clerk. This alternative meets the evaluation criteria and provides additional assurances for non-repudiation. Primary implementation issues include: (1) increased responsibility for the Clerk to manage and maintain a new system/technology; (2) changes to business process as a result of the implementation of OCR/ICR and workflow technologies; and (3) the appropriateness of implementing a PKI infrastructure specifically for the FD and LDA applications while a need for a House-wide PKI infrastructure may exist in the future.

The detailed methodology and results of this task can be found in Exhibit 4, *Feasibility Study*.

### **Cost-Benefit Analysis**

The purpose of the cost-benefit analysis was to analyze the viable system alternatives detailed in the feasibility study and examine the costs and benefits for implementing each alternative. The cost-benefit analysis included: (1) a cost analysis of the existing system and each alternative; (2) a cost sensitivity analysis to analyze the impact of changes in assumptions on the cost differences of the alternatives; and (3) an analysis of qualitative (or non-quantitative) factors.

### **Cost Analysis**

Figure 3: Existing System and Alternative Cost Analysis on the following page presents a summary of the non-recurring and recurring cost estimates for the existing system and the four viable system alternatives. The figure presents five-year total cost estimates discounted using a present value calculation to provide overall five-year lifecycle cost estimates of the existing system and each alternative.

As described in Exhibit 4, *Feasibility Study*, the alternatives build upon each other in terms of functionality and cost. For example, the estimated costs and functionality of the Imaging/Workflow alternative are included in all four alternatives. Additionally, the estimated costs and functionality for electronic filing in the Imaging/Workflow with Electronic Filing with Basic Encryption alternative are included in all remaining alternatives. The alternatives with PKI functionality differ only in terms of the estimated costs of outsourcing the PKI function versus maintaining the function in-house (by the Clerk).

Cost Factor	Existing System	Alternative 1	Alternative 2	Alternative 3	Alternative 4
		Imaging/Workflow System	Imaging/Workflow, w/Electronic Filing and Basic Encryption	Imaging/Workflow, w/Electronic Filing, and PKI (Outsourced)	Imaging/Workflow, w/Electronic Filing, and PKI (In-house)
<b>1. Non-Recurring Costs</b>					
Conversion/Testing	\$0	\$20,000	\$20,000	\$28,000	\$32,000
Software Integration/Customization	\$0	\$206,000	\$306,000	\$306,000	\$620,000
Hardware Purchase	\$0	\$77,000	\$95,000	\$107,000	\$107,000
Software Purchase	\$0	\$80,000	\$150,000	\$150,000	\$749,000
Training	\$0	\$5,000	\$11,000	\$14,000	\$41,000
CA Set-Up/Initialization	\$0	\$0	\$0	\$120,000	\$0
<b>Total Non-Recurring Costs</b>	<b>\$0</b>	<b>\$388,000</b>	<b>\$582,000</b>	<b>\$725,000</b>	<b>\$1,549,000</b>
<b>2. Recurring Costs</b>					
<b>Personnel Salaries and Fringe Benefits</b>					
Legislative Resource Center (Forms Processing)	\$2,335,000	\$2,078,000	\$2,078,000	\$2,078,000	\$2,078,000
Legislative Computer Systems (Computer Support)	\$126,000	\$483,000	\$839,000	\$839,000	\$1,195,000
House Information Resources (Mainframe Support)	\$60,000	\$0	\$0	\$0	\$0
<b>Hardware (Lease and Maintenance)</b>					
Mainframe Costs	\$126,000	\$0	\$0	\$0	\$0
OSAR Optical Disc Storage Maintenance	\$134,000	\$0	\$0	\$0	\$0
Other Hardware Maintenance	\$2,000	\$11,000	\$22,000	\$29,000	\$29,000
Scanner License/Maintenance	\$107,000	\$0	\$0	\$0	\$0
New Scanner License/Maintenance	\$0	\$23,000	\$23,000	\$23,000	\$23,000
New Optical Disc Storage Maintenance	\$0	\$3,000	\$3,000	\$3,000	\$3,000
<b>Software (License and Maintenance)</b>					
Image System Software License/Maintenance	\$7,000	\$0	\$0	\$0	\$0
RS-6000 Servers License/Operating System	\$34,000	\$0	\$0	\$0	\$0
Other Software License/Maintenance	\$47,000	\$26,000	\$69,000	\$69,000	\$69,000
PKI License/Maintenance	\$0	\$0	\$0	\$0	\$890,000
New Imaging System Maintenance	\$0	\$39,000	\$39,000	\$39,000	\$39,000
<b>External Vendor Services</b>					
PKI Vendor Hosting	\$0	\$0	\$0	\$305,000	\$0
<b>Total Recurring Costs</b>	<b>\$2,978,000</b>	<b>\$2,663,000</b>	<b>\$3,073,000</b>	<b>\$3,385,000</b>	<b>\$4,326,000</b>
<b>Total Estimated Costs</b>	<b>\$2,978,000</b>	<b>\$3,051,000</b>	<b>\$3,655,000</b>	<b>\$4,110,000</b>	<b>\$5,875,000</b>

Figure 3: Existing System<sup>6</sup> and Alternative Cost Analysis

The results of the cost analysis indicate that the estimated costs to implement each of the alternative systems are more expensive than maintaining the existing system over the next five year period. However, the alternatives do provide additional functionality over the existing system and better meet the criteria defined in this evaluation, as presented in Exhibit 4, *Feasibility Study*.

The total estimated costs for **Alternative 1: Imaging/Workflow System** are slightly higher than the existing system over the five-year period, primarily because of the non-recurring implementation costs. The recurring costs of the Imaging/Workflow System are less than the

<sup>6</sup> The total estimated costs for the existing system in this evaluation includes the costs associated with maintaining the FD and LDA applications as they are structured today. Because of the eventual migration off of the mainframe, the Clerk has investigated pursuing a solution that will serve during the interim between the time the applications are migrated off the mainframe and the time that the replacement solution for the FD and LDA applications are implemented. The potential interim solution involves porting the mainframe component of the FD and LDA application to a RS-6000 environment. The up-front costs (non-recurring) associated with this include approximately \$360,000 for hardware and software components. In addition, the potential recurring costs for the interim solution can be approximated as those attributed to the current mainframe component of the FD and LDA application (approximately \$126,000).

existing system recurring costs. For this alternative, we estimated that benefits would be achieved through lower recurring hardware and software maintenance costs.

The estimated costs for **Alternative 2: Imaging/Workflow System with Electronic Filing with Basic Encryption** are higher than the existing system, primarily because of the non-recurring implementation costs and the slightly higher recurring costs. For this alternative, we estimated that benefits would be achieved through lower labor costs (in terms of salaries and fringe benefits) for forms processing. However, we estimated that additional labor costs would be incurred for computer support due to the additional electronic filing functionality.

The estimated costs for both **Alternative 3: Imaging/Workflow System with Electronic Filing and an Outsourced PKI** and **Alternative 4: Imaging/Workflow System with Electronic Filing and an In-House PKI** are significantly higher than the existing system. Both alternatives require significant non-recurring implementation costs and the recurring costs are higher than the existing system. The cost estimates for the in-house PKI alternative are significantly higher than the outsourced PKI alternative due to the additional staff resources, and software license and maintenance costs required.

### **Cost Sensitivity Analysis**

We conducted a sensitivity analysis on the estimated costs (non-recurring and recurring) for the four viable alternatives analyzed in this evaluation. The objective of the sensitivity analysis was to analyze changes to assumptions to determine the impact on the overall cost of the alternatives. We developed the following two scenarios:

**Electronic Filing Efficiency Gains.** With the introduction of electronic filing capabilities, efficiencies may be realized with regards to the processing of the FD and LDA submissions. These efficiencies would occur primarily because of a reduction in hard copy form submissions. The extent of the efficiencies would primarily depend on the number of filers that choose to file electronically. To analyze the potential impact of efficiencies from electronic filing on the cost of the alternatives, we decreased the personnel salaries and fringe benefits cost factor associated with forms processing (LRC) for the electronic filing alternatives. The LRC salaries and fringe benefits cost factor was reduced by a range of percentages based on the corresponding percentage of filers who submit FD and LDA forms electronically. For the purposes of this analysis, we assumed a straight-line decrease in LRC forms processing staff costs, proportional to the percentage of respondents who submit electronically. Figure 4: Cost Sensitivity Analysis - Range of Electronic Filing Efficiency Gains below depicts the impact of the range of electronic filing percentages on the LRC forms processing staff costs of \$2,078,000 if electronic filing was not an alternative.

Percent of Electronic Filers	100%	75%	50%	25%	0%
Estimated Reduction in LRC Personnel Costs	50%	37.5%	25%	12.5%	0%
Total LRC Personnel Costs	\$1,039,000	\$1,319,530	\$1,558,500	\$1,818,250	\$2,078,000
(Cost Savings) Based on Electronic Filing	\$1,039,000	\$758,470	\$519,500	\$259,750	\$0

Figure 4: Cost Sensitivity Analysis - Range of Electronic Filing Efficiency Gains

- Increased Transition Costs.** We gathered costs information from vendors based on the high-level business needs associated with the four viable alternatives noted in this evaluation. However, these costs may differ from actual implementation costs due to the specific vendor chosen and the detailed requirements of the alternative. Therefore, we developed a scenario to examine the impacts of significantly higher implementation costs on each alternative. We increased the total transition costs associated with the four alternatives by 50 percent to represent a scenario in which the up-front costs to implement the alternatives are significantly more expensive. Figure 5: Cost Sensitivity Analysis - Transition Cost Increases details the impact of the cost increases on the alternatives.

Total Non-Recurring Cost Factor	Existing System	Alternative 1	Alternative 2	Alternative 3	Alternative 4
		Imaging/Workflow System	Imaging/Workflow System w/ Electronic Filing with Basic Encryption	Imaging/Workflow System w/ Electronic Filing with Outsourced PKI	Imaging/Workflow System w/ Electronic Filing with In-house PKI
Baseline Study Results*	\$0	\$388,000	\$582,000	\$725,000	\$1,549,000
Transition Cost Increase Scenario	\$0	\$582,000	\$873,000	\$1,087,500	\$2,323,500
<b>Difference</b>	\$0	\$194,000	\$291,000	\$362,000	\$774,500

Figure 5: Cost Sensitivity Analysis - Transition Cost Increases

\* From Figure 3: Existing System and Alternative Cost Analysis

### Qualitative Factor Analysis

In addition to the cost analysis and sensitivity analysis, we performed an assessment of qualitative, or non-quantifiable, factors for the system alternatives. The qualitative analysis was intended to provide additional evaluation criteria to analyze the alternatives. The qualitative factors analyzed were: (1) stakeholder needs and constraints, (2) management control, (3) security risk, (4) commercial acceptance, (5) organizational impact, and (6) filing community impact. The primary results of the qualitative analysis are:

- Stakeholder Needs and Constraints.** The Imaging/Workflow alternative achieves all of the identified stakeholder needs and constraints, with the exception of electronic filing. The remaining three alternatives satisfy all user needs and constraints.
- Management Control.** The outsourcing of PKI would result in the Clerk relinquishing some control over the issuance of digital certificate to respondents. However, the in-house PKI alternative keeps management control over the issuance of certificates within the ultimate control of the Clerk.

- **Security Risk.** The use of electronic filing introduces new needs to protect the confidentiality, integrity, availability, and authentication of the data for filers.
- **Commercial Acceptance.** The use of electronic filing and PKI technology has limited commercial acceptance because the technology is still relatively immature.
- **Organizational Impact.** All of the alternatives would require significant changes to the Clerk's business processes with regard to the processing of FD and LDA forms.
- **Filer Community Impact.** The use of electronic filing would allow filers to avoid the completion of hard copy forms. However, the use of PKI would require additional steps on the part of filers to apply and use certificates and keys.

The detailed methodology and results of this task can be found in Exhibit 5, *Cost-Benefit Analysis*.

### III. RECOMMENDED ACTIONS

The results of this study indicate that each of the alternatives examined in the evaluation are functionally and technically viable and justify the Clerk initiating a project to replace the existing systems. Because each alternative is viable and the cost differentiation across the alternatives are minor in comparison to improved efficiencies and services to stakeholders, a recommendation to implement a specific alternative is not provided. However, recommended steps for utilizing the results of the evaluation are provided. The recommended steps are categorized as:

- **Immediate.** Recommended actions that should be implemented or commenced as soon as possible, prior to initiating actions to replace the existing system.
- **System Planning, Development, and Implementation.** Recommended actions that should be taken or considered during the system planning, development, and implementation process.

The following discussion presents the specific recommendations for each of the above categories:

#### Immediate

The following recommendations should be implemented immediately.

- **Implement Recommended Safeguards.** As indicated in Exhibit 3, *Risk Assessment*, there are potential threats to the FD and LDA applications that could be resolved with the implementation of security safeguards. The Clerk should examine the recommended safeguards presented in the risk assessment to identify ones that can be implemented immediately to mitigate potential threats to the data and related assets of the FD and LDA applications.
- **Organize a FD/LDA Project Team.** The success of implementing a new system would greatly depend on the individuals identified and dedicated to this project. A project manager

should be assigned who would be directly responsible and accountable for the success of the project.

- **Develop a Work Plan.** The success of managing and executing large-scale projects greatly relies on a sound work plan. To assist the project manager in managing and executing the migration of the mainframe applications, we suggest that a comprehensive work plan be developed. The work plan should serve as a master plan that allows the project manager to monitor progress and facilitate the reporting to the Clerk and Committee on House Administration (CHA). The work plan should identify planning, implementation, and post-implementation tasks, including the phases of the SDLC policy. The time frames for the completion of the tasks should be based on the level of effort required to complete the tasks and the available resources.
- **Establish a Project Budget.** In order to ensure the system solution and implementation resources can be procured in a timely manner, the Clerk's Office should develop a project budget. The cost estimates in this evaluation can be used as a basis for budget planning for assessing the potential costs of the implementation of the system solution. However, the Clerk should be prepared to include additional costs once the system application and components have been chosen subsequent to developing the detailed requirements for the system. In addition, the Clerk may need to factor additional costs due any requirements for contractor support in implementing the solution in the event Clerk resources are not available to support the project.

### **System Planning, Development, and Implementation**

The following recommendations should be considered during planning, development, and implementation of the replacement system for the FD and LDA applications:

- **Conduct a Business Process Analysis to Determine Benefits of OCR/ICR Technologies.** Although the use of OCR/ICR technologies is feasible, the Clerk should analyze the specific uses of the technologies, and the impact on the business processes. It is critical to determine how these technologies would be specifically used prior to investment.
- **Assess Legal Implications and Acceptability of Electronic Filing.** The legal issues surrounding the use of electronic filing of FD and LDA submissions involve non-repudiation and the acceptability of digital information in a court of law. Research should be undertaken to derive conclusions of the appropriateness of using electronic filing prior to investment in this technology.
- **Determine Use and Acceptance of Electronic Filing by FD and LDA Filers.** The use and acceptance of electronic filing by FD and LDA filers is currently unclear. In Canada, approximately 90 percent of lobbyists submit information electronically. However, the Canadian Government assesses significant user fees to lobbyists who submit paper forms. Although Internet technologies have gained wide acceptance within the U.S., it is unclear to what extent FD and LDA filers would file using electronic methods. The Clerk should, at a



minimum, survey FD and LDA filers to gauge acceptance and usage prior to investing in electronic filing technologies.

- **Determine House-Wide Requirements for Public Key Infrastructure.** This evaluation includes an alternative for implementing PKI within the Clerk specifically for the FD and LDA applications. However, the House should consider its requirements for PKI for other uses within the House prior to implementing this technology solely within the Clerk. The PKI model presented in this evaluation could be used House-wide, with appropriate changes. For example, if a House-wide PKI is implemented, the Clerk may not be the appropriate office to manage the public and private key distribution. However, the implementation of a system solution that utilizes electronic filing with PKI could serve as a pilot for a House-wide assessment of the use of such technologies in other areas of the House.
- **Make Decisions Regarding Implementation of Alternatives.** Although the alternatives presented in this evaluation could be implemented in phases, the Clerk should make decisions regarding which alternatives to implement prior to beginning systems development.
- **Use the House's Systems Development Lifecycle Methodology.** The Clerk should follow the House's SDLC policy during systems planning, development, and implementation. This step is critical to ensuring a successful implementation.

### **Management Response**

On March 1, 1999, the Clerk agreed that the Legislative Systems Evaluation establishes reasonable parameters for determining information technology solutions for the high-level business needs associated with the FD and LDA applications (see Appendix). The Clerk agreed that the current application systems should be replaced as recommended and stated that the Office of the Clerk would follow the House SDLC Methodology. The response also included comments regarding: (1) implementing the recommended safeguards to mitigate the potential threats to FD and LDA applications, (2) the development of a FD/LDA project team, (3) the need to review the legal implications and acceptability of electronic filing, and (4) the need to select the most cost-effective and practical alternative at the earliest possible time.

### **Office of Inspector General Comments**

The Clerk's commitment to follow the SDLC policies adopted by the House is responsive to the issues discussed in this evaluation. Following the SDLC policy will minimize the developmental risk and provide the basis for an efficient and effective replacement for the FD and LDA applications. Furthermore, the Clerk's planned and completed actions, which address the potential threats identified during the risk assessment of the current FD and LDA operating environments will also mitigate the risks identified in this report.



**Exhibit 1**

**Exhibit 1**

**Application Overviews**



## **Application Overviews**

### **Table of Contents**

1.1.	Financial Disclosure (FD) .....	1
1.1.1	Input.....	3
1.1.2	Process .....	3
1.1.3	Output .....	4
1.1.4	Technical Information .....	4
1.2.	Lobby Disclosure Act (LDA).....	6
1.2.1	Input.....	7
1.2.2	Process .....	7
1.2.3	Output .....	8
1.2.4	Technical Information .....	8



## **Application Overviews**

This exhibit presents an overview of the Financial Disclosure (FD) and Lobby Disclosure Act (LDA) applications. The overview provides a brief description of the application's background and functionality. Specifically, the overview includes:

- A description of the legislation that the applications support.
- A description of the applications which identify the developer, the U.S. House of Representatives (House) office responsible for operating and maintaining the application, and the primary users of the applications.
- A description of the functionality of the applications which presents information on inputs, processes, and outputs.
- A table listing details for each application including the:
  - Application metrics.
  - Users/Customers.
  - Key inputs.
  - Key interfaces.
  - Key outputs.

In compiling the application overviews, a two step approach was followed to collect information. The two steps involved include:

- Interviewing House staff to collect information on the applications.
- Reviewing House documentation.

### **1.1. Financial Disclosure (FD)**

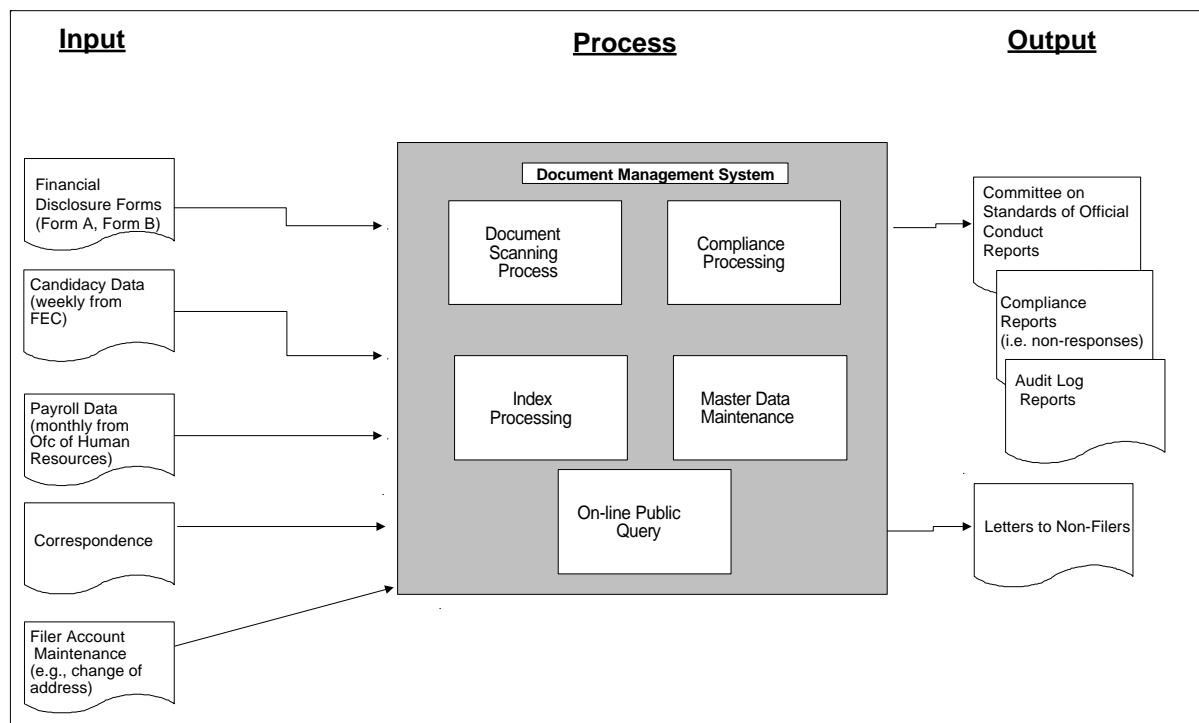
Title I of the Ethics in Government Act requires candidates for the House to file a personal financial disclosure statement with the Office of the Clerk (Clerk). In accordance with the Act, a House candidate that has raised or spent more than \$5,000 for his or her campaign is required to file a financial disclosure statement. In general, the statement must be filed within 30 days after the individual raises or spends the \$5,000, or on or before May 15 of the calendar year, in which he or she raises or spends \$5,000, whichever is later. There are various other individuals who must also file financial disclosure statements with the Clerk. House employees who, for at least sixty days, occupy a position for which the basic pay is equal to or greater than 120 percent of the minimum rate of basic pay for the GS-15 salary grade and covered employees of the Architect of the Capitol, U.S. Botanic Gardens, Congressional Budget Office, Government Printing Office, and Library of Congress are also required to file.

The Clerk manages the flow of FD submissions, using the FD application to manage the documents and relevant filer correspondence. The application consists of two components —



FileNet, a commercially available software application operated and maintained by the Clerk, and a mainframe-based application developed, operated, and maintained by the House Information Resource (HIR) office. The FileNet software is used to scan hard-copy reports, accept querying criteria for viewing by the general public, and display the report images. The mainframe-based application is used to generate queries and record dates for image indexing and processing. The primary user of the application is the Clerk's Legislative Resource Center (LRC).

Figure 1.1: FD Application Overview below presents an overview of the inputs, business processes, and outputs associated with the FD application. This figure depicts the flow of information from the input of data on the left, to application processing in the center, to outputs on the far right. A brief description of the inputs, processes, and outputs are presented following the figure.



*Figure 1.1: FD Application Overview*

## **Input**

The inputs to the FD application include the following:

- **Financial Disclosure Form (Form A and Form B).** Form A, used for submissions by Members of the House and House Officers, and Form B, submitted by House staff and potential candidates for the House, are mailed or delivered in person to the LRC by filers and subsequently scanned into the FD application. Forms A and B are mailed to filers upon request or are available to filers in downloadable format on the Clerk's website.
- **Candidacy Data.** The Federal Election Commission (FEC) reports to the Clerk, a list of all candidates who have reached the \$5,000 income and spending threshold. This information is manually keyed into the FD application from the hardcopy reports received from the FEC. The entry of this information into the FD application facilitates the tracking of all individuals subject to filings under the Ethics in Government Act.
- **Payroll Data.** The House Office of Human Resources (OHR) reports to the Clerk, a list of all House employees who met or exceeded the specified salary requirements as noted by the Ethics in Government Act. This information is manually keyed into the FD application from the hardcopy reports received from the OHR. The entry of this information into the FD application facilitates the tracking and compliance of all individuals subject to the Ethics in Government Act.
- **Correspondence.** Various letters of correspondence are received by the LRC from filers. The correspondence is scanned into the FD application.
- **Filer Account Updates.** Filer account updates (e.g., change of address or name) are received from filers. The updates are manually entered into FD to update master records requested by filers.

## **Process**

Listed below are the processes of the FD application.

- **Scanning.** Incoming FD forms and miscellaneous filer correspondence is scanned by the Clerk's FileNet application. Once the document is scanned, FileNet displays the document to the operator for quality control inspection. If the document is scanned properly, the document image is committed to permanent storage.
- **Indexing.** The operator who reads the information from the scanned image manually inputs information from the FD forms into the mainframe database index. Specific index information entered into FileNet during the scanning phase is automatically passed to the mainframe database.
- **Compliance Processing.** Compliance processing is not automated in the FD application. The LRC's role in compliance processing is to determine the response/non-response status of those required to file FD submissions. This is done by querying the FD application database on-line to review FEC and OHR data to determine filing compliance. All other compliance

processing with regards to the information contained in the FD submissions is performed by the Committee on Standards of Official Conduct.

- **Master Data Maintenance.** Master data maintenance involves the management of all data associated with the FD application. Data includes FD form images, form index information and information provided from external sources (i.e., FEC and OHR).
- **On-line Public Query.** The general public and other application stakeholders may query FD documents and associated information on-line in the LRC public area. A number of workstations with large screen monitors and printing capability are available during LRC business hours for public on-line querying.

## **Output**

The outputs of the FD application include the following:

- **Committee on Standards of Official Conduct Reports.** Various ad-hoc reports are generated for use by the Committee on Standards of Official Conduct when reviewing FD submissions.
- **Compliance Reports.** Response/non-response reports are generated using the data contained in the FD database. The reports assist LRC administrators in their efforts in identifying those filers not meeting the requirements of the Act.
- **Audit Log Reports.** Audit log reports are generated that detail relevant FD system usage.
- **Letters and other correspondence.** Form letters are generated via a word processing mail merge file. They are subsequently mailed to those filers not in compliance.

## **Technical Information**

Figure 1.2: FD Application Technical Information on the following page presents additional technical and application metric information for the FD application.

<b>Application Metrics</b>		
<b>Element</b>	<b>Description</b>	
Technology Platform	IBM CMOS mainframe; FileNet Imaging system maintained on (2)RS-6000s; and OSAR Optical Disk storage system	
Processing Mode	On-line transaction processing	
Number of Lines of Code	FileNet – 22 files comprised of 28,688 lines Mainframe – 225 modules comprised of 22,500 lines	
Data Storage	Mainframe – Approximately 151 MB; OSAR – Approximately 15 GB in use (2.3 and 7 GB disks available)	
Number of records in database	Approximately 53,000	
Documents scanned per year	Approximately 3,000	
Handwritten documents received (66.5% of total)	9%	Members of Congress
	23%	Congressional Candidates
	17%	Principal Assistants
	24%	House Employees
	27%	Library of Congress
Typewritten documents received (33.5% of total)	45%	Members of Congress
	15%	Congressional Candidates
	17%	Principal Assistants
	15%	House Employees
	8%	Library of Congress
<b>Users/Customers</b>		
<b>Element</b>	<b>Description</b>	
Number of Filers	2,990	
Key application users	House Members, House Employees, Candidates, Library of Congress Employees, Botanical Gardens Employees, Government Printing Office Employees, Congressional Budget Office, Architect of the Capitol Employees, General Public, Public Interest Groups, Press Corp.	
<b>Key Inputs</b>		
<b>Input</b>	<b>Source</b>	
FileNet Images	Financial Disclosure-Form A and Form B.	
Document index data	Via manual key entry from information contained in the hardcopy document.	
<b>Key Interfaces</b>		
<b>System</b>	<b>Description</b>	
FileNet	FileNet sends query criteria to the mainframe and the mainframe application sends back the query results.	
<b>Key Outputs</b>		
<b>Output</b>	<b>Description</b>	
Letters	Letters sent to non-filers.	

Figure 1.2: FD Application Technical Information

## 1.2. Lobby Disclosure Act (LDA)

The LDA of 1995 requires lobbying firms and organizations to register and file reports of their lobbying activities with the Secretary of the Senate and the Clerk of the House. A registrant must file a report semi-annually no later than 45 days after the end of the first day of January and the first day of July. Registrants call the LRC to request the LD-1 form if they are new registrants or the LD-2 form if they are submitting their semi-annual report. The forms are also available for download from the Clerk's web site.

The Clerk is responsible for managing the flow of paperwork generated by LDA registrants for the House and enforcing registrant compliance with the Act. The Clerk uses the LDA application to manage the Lobby Act documents and track compliance. The application consists of two components: FileNet, a commercially available software application operated and maintained by the Clerk; and the mainframe-based application developed, operated, and maintained by HIR. FileNet software is used to scan hard-copy reports, accept querying criteria for viewing by the general public, and display the report images. The mainframe-based application is used to generate queries and record dates for image indexing and processing. The primary user of the application is the Clerk's LRC.

Figure 1.3: Lobby Disclosure Act Application Overview on the following page presents an overview of the inputs, processes, and outputs associated with the LDA application. This figure depicts the flow of information from the input of data on the left, to application processing in the center, to outputs on the far right. A brief description of the inputs, processes, and outputs are presented following the figure.

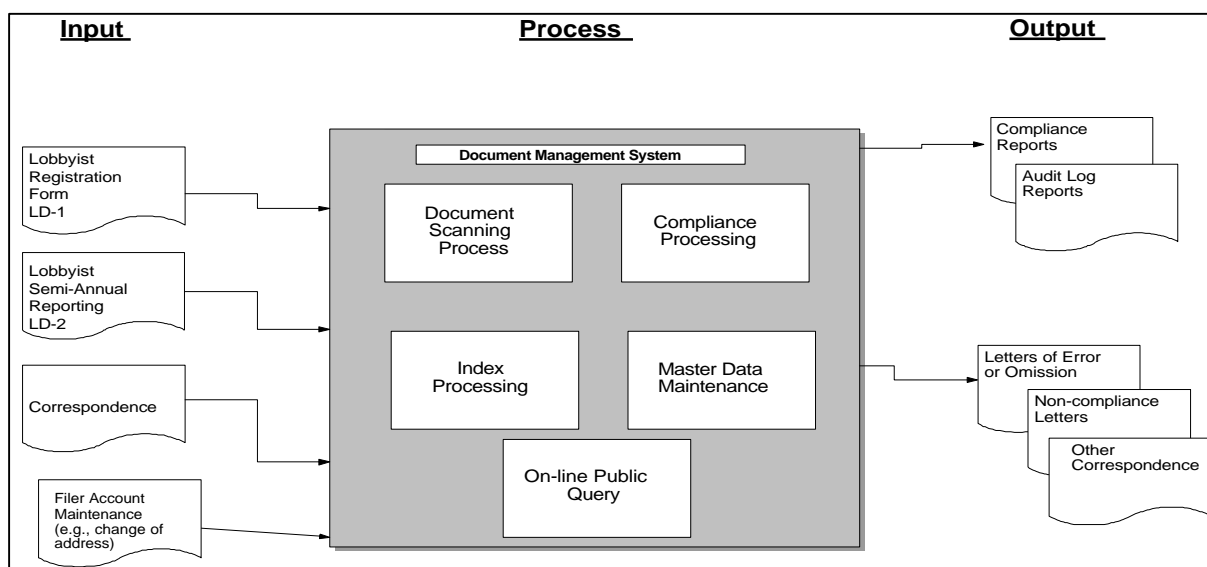


Figure 1.3: Lobby Disclosure Act Application Overview

### **1.2.1 Input**

The inputs to the LDA application include the following:

- **Lobbying Registration and Report Forms (Form LD-1 and LD-2).** Form LD-1 (for initial registration) and LD-2 (for semi-annual reporting) are sent to filers upon request or are available to filers in downloadable format on the Clerk's website. Registrants send their completed forms to the Clerk via mail on a semi-annual basis. Form LD-1 and LD-2 are subsequently scanned into the LDA application.
- **Correspondence.** Various letters of correspondence are received by the LRC from registrants. The correspondence is scanned into the LDA application.
- **Filer Account Updates.** Filer account updates (e.g., change of address or name) are received from registrants. The updates are manually entered into the LDA application to update master records requested by registrants.

### **1.2.2 Process**

Listed below are the processes of the Lobby Act application.

- **Scanning.** Incoming LDA forms and miscellaneous registrant correspondence are scanned into the Clerk's FileNet application. Once the document is scanned, FileNet displays the document to the operator for quality control inspection. If the document is scanned properly, the document image is committed to permanent storage.
- **Indexing.** The operator who reads the information from the scanned image manually inputs information from the LDA forms into the mainframe database index. Specific index information entered into FileNet during the scanning phase is automatically passed to the mainframe database.
- **Compliance Processing.** Compliance processing is not automated in the LDA application. However, LRC administrators use the LDA query function to evaluate registrant information. If there are errors or omissions such as missing figures for lobbying expenses or erroneous lobbying topic codes, a letter is generated and mailed to the registrant.
- **Master Data Maintenance.** Master data maintenance involves the management of all data associated with the LDA application. Data includes LDA form images and form index information.
- **On-line Public Query.** The general public and other application stakeholders may query LDA documents and associated information on-line in the public area of the LRC. A number of workstations with large screen monitors and printing capability are available during LRC business hours for public on-line querying.

### **1.2.3 Output**

The outputs to the LDA application include the following:

- **Compliance Reports.** Various compliance reports are generated using the data contained in the LDA database. The reports assist LRC administrators in their efforts in identifying those registrants not meeting the requirements of the Act.
- **Audit Log Reports.** Audit log reports are generated that detail relevant LDA system usage.
- **Letters and other correspondence.** Form letters are generated via a word processing mail merge file. They are subsequently mailed to those registrants not in compliance or filers who submitted forms with errors or omissions.

### **1.2.4 Technical Information**

Figure 1.4: LDA Application Technical Information on the following page presents additional technical and application metric information for the LDA application.

<b>Application Metrics</b>	
<b>Element</b>	<b>Description</b>
Technology Platform	IBM CMOS mainframe; FileNet Imaging system maintained on (2)RS-6000s; OSAR Optical Disk storage system
Processing Mode	On-line transaction processing
Number of Lines of Code	FileNet – 22 files comprised of 28,688 lines of code Mainframe – 300 modules comprised of 65,000 lines
Data Storage	Mainframe – Approximately 147.5 MB; OSAR – Approximately 82.5 GB in use (2.3 and 7 GB disks available)
Number of records in each database	Registrants – 24,655      Clients – 68,284 Lobby Table – 3,924      Reports- 451,924 Employees – 52,458      Letters – 75,015 Directory – 5,616
Documents scanned per year	Approximately 35,000 pages
Percentage of handwritten documents received	12%
Percentage of typewritten documents received	88%
<b>Users/Customers</b>	
<b>Element</b>	<b>Description</b>
Number of Filers	Active Registrants – 3,727; Active Clients – 11,616
Key application users	Lobbyists, LRC, General Public, Public Interest Groups, Press Corp.
<b>Key Inputs</b>	
<b>Input</b>	<b>Source</b>
FileNet Images	Submitted registration documents and reports.
Document index data	Via manual key entry from information contained in the hardcopy document.
<b>Key Interfaces</b>	
<b>Interface</b>	<b>Description</b>
FileNet/LDA link	Data is scraped after FileNet document scanning and loaded into the LDA database residing on the mainframe.
<b>Key Outputs</b>	
<b>Output</b>	<b>Description</b>
Letters	Letters of errors or omissions sent to registrants.
Reports	List all lobbyists and their clients.

*Figure 1.4: LDA Application Technical Information*





**Exhibit 2**

**Needs Statement**



**Needs Statement**

**Table of Contents**

2.1. The Clerk's Mission ..... 1

2.2. Deficiencies ..... 1

2.3. New or Changed Program Needs ..... 4

2.4. High-Level Business Needs ..... 4

2.5. Opportunities for Increased Economy and Efficiency ..... 4



## **Needs Statement**

This exhibit presents the high-level business needs of the Financial Disclosure (FD) and Lobby Disclosure Act (LDA) applications.<sup>7</sup> The purpose of this needs statement is to identify deficiencies in existing capabilities, new or changed program needs, and overall needs of these two applications as they relate to the Office of the Clerk's (Clerk) mission.<sup>8</sup> The needs statement also identifies opportunities for increased economy and efficiency and provides justification for exploring alternative solutions.

### **2.1. The Clerk's Mission**

The Clerk is responsible for preserving, and making available to the public, records of the U.S. House of Representatives (House). The Clerk is the official depository for various published documents originated and produced by the House and its committees, for the historical records of the House, and for public disclosure of documents made available under various House Rules and Public Laws. The mission of the Clerk was used as a framework for defining the high-level needs for the purpose of identifying alternative system solutions to the FD and LDA applications. As presented in Exhibit 1, *Application Overview*, the FD and LDA applications support the Clerk's mission by providing public access to the disclosures submitted by various parties, as mandated by law.

### **2.2. Deficiencies**

Through discussion with the Clerk users and work performed in developing Exhibit 3, *Risk Assessment*, deficiencies in the current FD and LDA applications were identified. These deficiencies were later used as a basis for defining high-level needs used to identify alternative solutions. The deficiencies that affect both systems, and deficiencies specific to the FD and LDA applications are listed below.

#### **Both Systems**

- Substantial amount of manual entry and reconciliation during forms processing. Extensive effort is expended re-keying information that already resides in the system (i.e., annual FD database recompilation effort).
- General dissatisfaction with the current FileNet imaging system due to the increasing costs to maintain and enhance the current system, as well as the level of vendor support provided.

#### **Financial Disclosure Act (FD)**

---

<sup>7</sup> For the purposes of this evaluation, a high-level business need is an identified requirement asserted by application users and administrators, which addresses the mission of the Clerk. The high-level business needs presented in this evaluation are not intended to serve as functional requirements. The functional requirements are addressed in the analysis phase of the U.S. House of Representatives System Development Life Cycle Policy.

<sup>8</sup> The functionality of the FD and LDA applications is very similar. Therefore, this needs statement comprises the high-level needs for both applications.

- No automated data interfaces with external entities for the FD application. Interfaces with external agencies (i.e., Federal Elections Commission) would eliminate the need to manually key information currently provided in hard copy reports and would improve data integrity.

### **Lobby Disclosure Act (LDA)**

- Inefficient methods to delete, edit, and manipulate LDA data, which leads to an increase in manual reconciliation and the risk of human error. For example, redundant tasks are performed during the current LDA indexing process.
- LDA reminder notices are sent based upon lobbyist and client combinations. Therefore, if a lobbyist has 100 clients, the lobbyist receives 100 post card sized notices.

### **2.3. New or Changed Program Needs**

During discussions with the Clerk users, no foreseen new or changed program needs associated with the LDA and FD applications were identified. However, any new system alternatives must be flexible enough to allow efficient response to changes in system needs or general duties of the Clerk, without considerable rework of the system and associated business processes.

### **2.4. High-Level Business Needs**

This section details the high-level needs identified by the Clerk users and administrators to support the LDA and FD applications. Although many of the needs are expressed in terms of the current LDA and FD applications, consideration has been given to the future computing needs of the Clerk. The following list summarizes primary user's needs and the context of their importance as noted by Clerk management and administrators:

#### **Input**

- Ability to minimize the amount of manual data entry during both forms processing and the annual FD database compilation.
- Ability to receive information on individuals subject to FD reporting requirements through automated interfaces (e.g., Federal Elections Commission, Finance Office).

#### **Processing**

- Ability to automate the method through which reporting compliance is determined.
- Provide for the capability to destroy existing images within a specified time period, as required by law.

#### **Output**

- Ability to print reminder notices to non-filers in an efficient manner.
- Ability to generate letter of inquiry for LDA errors or omissions.
- Allow for high-speed printing from images using a user defined sort order.
- Ability to use commonly used graphical file formats that are compatible with various printers (e.g., LRC's high speed printer).

### **Query and Reports**

- Provide for flexible record query and reporting capabilities for both public and LRC staff use.

### **Storage**

- Ability to track forms from initial receipt to archive. Ability to link:
  - Individual hardcopy or electronic submissions.
  - System generated document and batch identification number.
  - Archive box storage ID.
- Ability to back up images and indices.
- Ability to maintain images in a non-proprietary format.

### **Technology**

- Provide for a network centric platform (client/server) for FD and LDA system and maintain hardware, software, and data within the Clerk's office.
- Ability to use Internet technologies.
- Allow for potential public access via the Internet.
- Allow for electronic filing and signature verification.

### **Application Controls and Security**

- Provide for system availability on a timely and consistent basis.
- Ability to prevent unauthorized access.
- Ability to restrict access to FD information before the official release to the general public.
- Ability to protect data during electronic filing, processing, and storage.
- Ability to authenticate the users of the FD application, including the identification of general public users, as mandated by law.



## **2.5. Opportunities for Increased Economy and Efficiency**

After review of the current state of the FD and LDA applications, several areas were identified that could provide opportunities for increased economy and efficiency to the Clerk's Office. The following have been identified as the key areas where economy and efficiency could be achieved:

- Improve level of service provided from the existing imaging system.
- Reduce labor expense through more efficient data input and forms processing methods.
- Improve ability to respond to changes in FD and LDA filing requirements in a more timely manner.
- Minimize inefficiencies associated with non-responses to LDA mass mailings.
- Provide an efficient hard-copy archive mechanism

**Exhibit 3**

**Risk Assessment**



**Risk Assessment**

**Table of Contents**

3.1 Methodology..... 1

    3.1.1 Threats ..... 2

    3.1.2 Data and Assets ..... 2

    3.1.3 Vulnerability ..... 3

    3.1.4 Risk Impact ..... 4

    3.1.5 Recommended Safeguards ..... 4

3.2. Risk Assessment Results..... 5

3.3. Risk Considerations for Alternate Solutions..... 12

    3.3.1 Network Centric Platform..... 12

    3.3.2 Electronic Filing and Digital Signature ..... 12



## **Risk Assessment**

This exhibit presents the risk assessment for the Financial Disclosure (FD) and Lobby Disclosure Act (LDA) applications. The risk assessment identifies threats to data and assets, the potential impact of those threats, system vulnerabilities and existing safeguards, and the current internal control and security environment of the systems. Specifically, the risk assessment includes:

- A description of the methodology used to perform the risk assessment.
- The identification of the threats to data and assets, the vulnerabilities related to the threats, the risk impact of the threats, and recommended safeguards to mitigate the threats.
- A brief discussion of risk considerations for potential alternative system solutions for the application.

The results presented in this exhibit also served as input to Exhibit 2, *Needs Statement* in identifying the current deficiencies of the FD and LDA applications and new needs for potential replacement systems.

### **3.1. Methodology**

The purpose of the risk assessment was to identify threats to data and assets, the potential impact of those threats, system vulnerabilities, and existing safeguards. Using an internal control and security diagnostic tool, we gained an understanding of the current vulnerabilities and related safeguards. Information for the diagnostic tool was gathered through observations made during walkthroughs of the systems and facilities, and from interviews with the Office of the Clerk (Clerk) and the House Information Resources (HIR) office. Due to the scope and purpose of the risk assessment, we have not conducted any detailed testing and validation typically completed during a detailed internal controls and security review or audit. The diagnostic tool used was comprised of questions covering the following areas listed below:

- Information security policies and procedures.
- Security administration and management.
- Business continuity planning.
- Application level controls.
- System level controls.
- Network level controls.
- Internet security.

The data collected from the diagnostic tool was analyzed with respect to the following risk assessment components:

- Threats.
- Data and assets.
- Vulnerabilities.

- Risk impact.
- Potential safeguards.

The following sections describe each risk assessment component.

### **3.1.1 Threats**

A threat can be defined as a person or event that can potentially cause destruction or loss to something valuable. For example, an unauthorized user who attempts to access information they are not privy to is a threat. Threats may be categorized as follows:

- **Events.** Events, such as natural disasters, that can often have severe consequence on the data.
- **External threats.** People who may attempt to access data from outside the system.
- **Internal threats.** People who may attempt to access data from inside the system. These people are authorized to access the system and may even have access to valuable data.

### **3.1.2 Data and Assets**

The following page lists the critical data and assets related to the FD and LDA applications that were examined in the risk assessment. Included in the listing is a qualitative value of the data.<sup>9</sup>

#### **Data**

- **FD and LDA Forms**

The FD and LDA applications allow filed FD and LDA forms to be made available for viewing by the general public. Physical forms submitted to the Clerk are scanned and indexed. The FD hardcopies are maintained and destroyed after six years, whereas the LDA hardcopies are archived first at the Cannon Building, then moved to the National Archives for storage.

Value of data – Both the physical forms and form images are mission critical in order to adhere with the spirit of the FD and LDA laws.

- **FD and LDA Application Indices**

Both the mainframe and FileNet components contain index data through which the FD and LDA digital images are accessible. The index uniquely identifies each filer's record and contains location information that is used by FileNet to retrieve document images. The FD application index includes Social Security Numbers for some House employees.

Value of data – Mission critical to locate images and archived physical documents. Social Security Numbers are extremely valuable to individual filers.

---

<sup>9</sup> Qualitative values are best used when attempting to identify where major problems exist. Since this risk assessment is being conducted as a first step towards justifying replacement alternatives, an in-depth detailed review is not necessary.

- **FD Query Activity Log**

The Ethics in Government Act requires that all individuals who access FD documents to identify themselves prior to viewing. The FD query activity log captures this information along with other user activities.

Value of data – Not mission critical, but required.

- **User Account Information**

ACF2<sup>10</sup> user account information, consisting of user ID and password combinations, allows users access to the mainframe component of FD and LDA. The account information is the primary means used to authenticate Clerk users and administrators. In addition to the mainframe accounts, there are accounts for the FileNet system, the Windows NT network, and the AIX operating system for the RS-6000 platform.

Value of data – Mission critical to protect the confidentiality, integrity, availability, and authentication of data.

## Equipment

- **Mainframe (located in HIR)**

The indices of both the FD and LDA digital images are located on the mainframe.

- **The Enterprise Network**

The current processing environment is located in facilities in the Cannon, Rayburn, and Ford House office buildings. The House's enterprise network (BUDnet) is the communications medium for the FD and LDA system.

- **Image Server (located in Legislative Computer Systems (LCS))**

After the FD and LDA forms are scanned into the workstation, they are transmitted to the FileNet Image Server for storage. Once digital images are on the FileNet Server, they must be indexed before they can be viewed via public access computers. Subsets of the mainframe index are also duplicated on the FileNet Server.

- **Personal Computers, Printers, and Scanners (located in Legislative Resource Center (LRC))**

The public uses workstations to retrieve and view FD and LDA documents. The document scanning process also relies upon workstations to run the FileNet client.

### 3.1.3 Vulnerability

---

<sup>10</sup> ACF2 is an access control software program that maintains and manages user ID and password combinations.



A vulnerability is defined as a weakness that can be exploited by a threat. For example, a flaw or deficiency in the system design, weak administrative policies and procedures, or weak physical security may increase the likelihood of a threat by permitting easier access to data. The more secure a computer system, the less vulnerable its data is to threats, or the less likely the threats can penetrate the computer system. Therefore, the magnitude of the threats is directly related to the vulnerabilities of the computer system. From a risk perspective, the greater the vulnerabilities, the greater the risks.

### **3.1.4 Risk Impact**

Four fundamental areas of risk related to data were examined in the risk assessment of the FD and LDA systems: confidentiality, integrity, availability, and authentication. The security fundamentals, consequences of compromises to the security fundamentals, and the related risk type of each are identified below.

- **Confidentiality.** Ensures that sensitive information is available only for the intended audience and that sensitive information is not disclosed to unauthorized individuals. The consequence of compromise includes public embarrassment or legal liability from unauthorized disclosure of sensitive and critical information.

RISK TYPE: Disclosure of confidential information.

- **Integrity.** Ensures that information is modified or changed only in a specified and authorized manner. The consequence of compromise includes loss of information or the creation of false information if critical data is accidentally or intentionally manipulated.

RISK TYPE: Modification of data.

- **Availability.** Ensures that systems operate promptly and service is not denied to authorized users. The consequence of compromise includes a disruption of operations due to inaccessible information.

RISK TYPE: Disruption of operations.

- **Authentication.** Ensures that only authorized users have access to the system. The consequence of compromise includes unauthorized access to sensitive information.

RISK TYPE: Impersonation of an individual's identity.

### **3.1.5 Recommended Safeguards**

Recommended safeguards are actions that can be implemented to minimize or eliminate potential security threats. The safeguards can be categorized as technical, administrative, and physical. The technical safeguards are system related and can be used as criteria when evaluating system alternatives. Administrative and physical safeguards are independent of any system solution. Therefore, the administrative and physical safeguards are ones that can be implemented as soon as possible to minimize security risk.

### **3.2. Risk Assessment Results**

Nine high-level threats were identified in the risk assessment to which the FD and LDA applications and their data may be vulnerable. These threats originate from events or people internal or external to the House. Listed below is a description of the threats.

#### **Events**

- **Acts of Nature.** Includes acts of nature such as flood, hurricane, tornado, earthquake, or lightning strike that have the potential to physically destroy documents or the House data centers located in the Cannon, Rayburn, or Ford buildings.
- **Acts of terrorism.** Includes various acts of violence against the House such as a bombing attack.
- **Data center environmental compromise.** Includes events affecting power supply, communications capabilities, or other environmental incidents, such as water leakage, within the building.
- **Software/hardware failure.** Includes the failure of system components.

#### **People**

- **Intentional acts by House staff.** Includes the threats posed by disgruntled or malicious House staff, including physical destruction of property, compromise of document integrity (to cause embarrassment to filer) or the insertion of malicious object code (to cause processing disruption).
- **Fraudulent filing.** Includes the threats of fraudulent filing by an authorized filer or someone masquerading as an authorized filer.
- **Misrepresentation of identity.** Includes general public users who do not accurately identify themselves while accessing imaged forms.
- **Human error.** Includes accidental acts by staff, including erroneous data entry or improper system or security administration (causing third party compromise of data).
- **Logical/physical penetration.** Includes system access (physical or logical) by unauthorized public users.

Figure 3.1: Summary of Risk Assessment Results on the following page provides a summary of the risk assessment results. It includes a detailed description of the threats, vulnerabilities, potential impact, and potential safeguards to minimize or eliminate the threats.

<b>Threat</b>	<b>Data and Assets Affected</b>	<b>Vulnerabilities</b>	<b>Risk Impact</b>	<b>Recommended Safeguards</b>
Acts of nature	<p>Data:</p> <ul style="list-style-type: none"> <li>Form images</li> <li>Index</li> <li>FD Query Activity Log</li> <li>User Account Information<sup>11</sup></li> </ul> <p>Equipment:</p> <ul style="list-style-type: none"> <li>LCS</li> <li>LRC</li> <li>HIR</li> </ul>	<p><i>No business continuity plan (BCP) within the Clerk.</i></p> <p><b>Observations:</b></p> <ul style="list-style-type: none"> <li>There is no comprehensive HIR/LCS BCP plan for the FD and LDA applications that has been circulated to staff in LCS or LRC. The LCS is currently drafting a BCP document. Testing of the BCP plan however, has never been performed. Additionally, there are no backups made of the FileNet document images.</li> </ul>	<p><b>Disruption -</b> Images and indices not available for period of time. The permanent destruction of the FileNet images is possible.</p>	<ul style="list-style-type: none"> <li>Develop, test, and implement a BCP.</li> <li>Develop, test, and implement document image backup procedures.</li> <li>Use an off-site storage facility consistent with the practices of HIR, to store and maintain tape and/or image platter backups.</li> </ul>
Acts of terrorism	<p>Data:</p> <ul style="list-style-type: none"> <li>Form images</li> <li>Index</li> <li>FD Query Activity Log</li> <li>User Account Info.</li> </ul> <p>Equipment:</p> <ul style="list-style-type: none"> <li>LCS</li> <li>LRC</li> <li>HIR</li> </ul>	<p><i>No BCP within the Clerk.</i></p> <p><b>Observations:</b></p> <ul style="list-style-type: none"> <li>There is no comprehensive HIR/LCS BCP plan for the FD and LDA applications that has been circulated to staff in LCS or LRC. The LCS is currently drafting a BCP document. Testing of the BCP plan however, has never been performed.</li> <li>Weak physical access controls for LCS data center.</li> </ul>	<p><b>Disruption -</b> Images and indices not available for period of time. The permanent destruction of the FileNet images is possible.</p>	<ul style="list-style-type: none"> <li>Develop, test, and implement a BCP.</li> <li>Develop, test, and implement document image backup procedures.</li> </ul>

Figure 3.1: Summary of Risk Assessment Results

<sup>11</sup> Refers to Mainframe ACF2 User ID, FileNet signon, and Windows NT account.

Threat	Data and Assets Affected	Vulnerabilities	Risk Impact	Recommended Safeguards
Acts of terrorism (continued)				<ul style="list-style-type: none"> <li>• Use an off-site storage facility consistent with the practices of HIR, to store and maintain tape and/or image platter backups.</li> <li>• Strengthen physical access controls (e.g., implement card key, guest sign-in and double-door access).</li> </ul>
Data center compromise-facilities	Data: <ul style="list-style-type: none"> <li>• Form images</li> <li>• Index</li> <li>• FD Query Activity Log</li> <li>• User Account Info.</li> </ul> Equipment: <ul style="list-style-type: none"> <li>• LCS</li> <li>• LRC</li> <li>• HIR</li> </ul>	<i>No BCP within the Clerk.</i> <b>Observations:</b> <ul style="list-style-type: none"> <li>• There is no comprehensive HIR/LCS BCP plan for the FD and LDA applications that has been circulated to staff in LCS or LRC. The LCS is currently drafting a BCP document. Testing of the BCP plan however, has never been performed.</li> </ul>	<b>Disruption -</b> Images and indices not available for period of time.	<ul style="list-style-type: none"> <li>• Develop, test, and implement a BCP.</li> <li>• Develop, test, and implement document image backup procedures.</li> <li>• Use an off-site storage facility consistent with the practices of HIR, to store and maintain tape and/or image platter backups.</li> </ul>

Figure 3.1: Summary of Risk Assessment Results

Threat	Data and Assets Affected	Vulnerabilities	Risk Impact	Recommended Safeguards
Software/Hardware failure	Data: <ul style="list-style-type: none"> <li>• Form images</li> <li>• Index</li> </ul>	<i>No BCP within the Clerk.</i> <b>Observations:</b> <ul style="list-style-type: none"> <li>• There is no comprehensive HIR/LCS BCP plan for the FD and LDA applications that has been circulated to staff in LCS or LRC. The LCS is currently drafting a BCP document. Testing of the BCP plan however, has never been performed.</li> </ul>	<b>Disruption -</b> Images and indices not available for period of time.	<ul style="list-style-type: none"> <li>• Develop, test, and implement a BCP.</li> <li>• Develop, test, and implement document image backup procedures.</li> <li>• Use an off-site storage facility consistent with the practices of HIR, to store and maintain tape and/or image platter backups.</li> </ul>
Intentional acts by House staff	Data: <ul style="list-style-type: none"> <li>• Form images</li> <li>• Index</li> <li>• FD Query Activity Log</li> <li>• User Account Info.</li> </ul>	<i>Lack of application and system software change control.</i> <b>Observations:</b> <ul style="list-style-type: none"> <li>• FileNet application administrators have direct access to the production environment. Changes to FileNet run-scripts or changes to source code are not formally documented or approved.</li> </ul>	<b>Modification-</b> Unauthorized add, change, or delete of list data may have adverse ramifications that affect data integrity.  <b>Disruption –</b> Staff may disable system if the BCP plan is not effective.	<ul style="list-style-type: none"> <li>• Grant access to users based upon job duties, where applicable.</li> <li>• Provide for segregation of duties through workflow functionality.</li> </ul>

Figure 3.1: Summary of Risk Assessment Results

Threat	Data and Assets Affected	Vulnerabilities	Risk Impact	Recommended Safeguards
Intentional acts by House staff (continued)		<p><i>Lack of integrated security administration.</i></p> <p><b>Observations:</b></p> <ul style="list-style-type: none"> <li>• A coordinated approach to application access security has not been implemented. Currently, HIR and LCS have overlapping security responsibilities. Also, there is no security officer to monitor and manage security.</li> </ul> <p><i>No quality controls present.</i></p> <p><b>Observations:</b></p> <ul style="list-style-type: none"> <li>• An individual who scans and indexes a document may also verify its correctness.</li> </ul>	<p><b>Impersonation</b> – Staff may impersonate system administrator.</p>	<ul style="list-style-type: none"> <li>• Improve application change control procedures using change control tools.</li> <li>• Appoint a security officer to monitor and manage security.</li> </ul>
Fraudulent filings	<p>Data:</p> <ul style="list-style-type: none"> <li>• Form images</li> <li>• Index</li> <li>• FD Query Activity Log</li> </ul>	<p><i>No validation procedures in effect.</i></p> <p><b>Observations:</b></p> <ul style="list-style-type: none"> <li>• Hand written signature is the only validation performed for FD and LDA forms. Verification of the signature is only performed when a complaint is filed by the public or filer.</li> </ul>	<p><b>Impersonation</b> – Incorrect or fraudulent information may embarrass the Clerk or original filer.</p>	<ul style="list-style-type: none"> <li>• No improvements recommended. Inherent safeguard is present. The filer who has been impersonated would likely detect fraud.</li> </ul>
Misrepresentation of identity of public users	<p>Data:</p> <ul style="list-style-type: none"> <li>• FD Query Activity Log</li> </ul>	<p><i>No manual or automated authentication of application users.</i></p> <p><b>Observations:</b></p> <ul style="list-style-type: none"> <li>• There are no manual procedures to check the identification of FD or LDA users. Neither application has the functionality to authenticate end users.</li> </ul>	<p><b>Impersonation</b> – The identity of the user may be fraudulent.</p>	<ul style="list-style-type: none"> <li>• Implement manual or automated authentication procedures that are consistent with the spirit of the EIGA and LDA. Example includes increased staff intervention with users that reduce the users ability to falsify their identity.</li> </ul>

Threat	Data and Assets Affected	Vulnerabilities	Risk Impact	Recommended Safeguards
Human error by staff	Data: <ul style="list-style-type: none"> <li>• Form images</li> <li>• Index</li> <li>• FD Query Activity Log</li> <li>• User Account Info.</li> </ul>	<p><i>Lack of application and system software change control. <b>Observations:</b></i></p> <ul style="list-style-type: none"> <li>• FileNet application administrators have direct access to the production environment. Changes to FileNet run-scripts or changes to source code are not formally documented or approved.</li> </ul> <p><i>No segregation of incompatible duties. <b>Observations:</b></i></p> <ul style="list-style-type: none"> <li>• An individual who scans a document may also verify its correctness.</li> </ul> <p><i>Application edits and validations need improvement. <b>Observations:</b></i></p> <ul style="list-style-type: none"> <li>• The FD application requires excessive manual data entry.</li> <li>• The application edits and validations need improvement to reduce inadvertent errors and to improve data integrity (e.g., pull down menus, strong error detection controls).</li> </ul> <p><i>The FD and LDA applications do not have strong query capabilities. <b>Observations:</b></i></p> <ul style="list-style-type: none"> <li>• The ability to detect data redundancy through precise database query functions is not present.</li> </ul>	<p><b>Modification –</b> Unintentional changes to data are possible.</p> <p><b>Disruption –</b> Denial of service possible by unintentional act.</p>	<ul style="list-style-type: none"> <li>• Grant access to users based upon job duties.</li> <li>• Provide for segregation of duties through workflow functionality.</li> <li>• Improve application change control procedures using change control tools.</li> <li>• Reduce redundant data entry.</li> <li>• Provide for strong application edits and validations.</li> <li>• Implement stronger and more precise query capabilities.</li> </ul>

Figure 3.1: Summary of Risk Assessment Results

Threat	Data and Assets Affected	Vulnerabilities	Risk Impact	Recommended Safeguards
Logical/physical penetration to data center by unauthorized public users	Data: <ul style="list-style-type: none"> <li>• Form images</li> <li>• Index</li> <li>• FD Query Activity Log</li> <li>• User Account Info.</li> </ul> Equipment <ul style="list-style-type: none"> <li>• LCS</li> <li>• LRC</li> <li>• HIR</li> </ul>	<i>Lack of integrated security administration; weak physical access security to data center.</i> <b>Observations:</b> <ul style="list-style-type: none"> <li>• A coordinated approach to application access security has not been implemented. Currently, HIR and LCS have overlapping security responsibilities. Also, there is no security officer to monitor and manage security.</li> <li>• Observed no card key access control or locks to LCS data center. Direct access door to hallway is alarmed but not activated (observed staff exiting door to hallway).</li> <li>• No physical access controls to registration and filings processing areas. These areas provide access to forms in both physical and electronic formats.</li> </ul>	<b>Disclosure -</b> Viewing of document images prior to release.  <b>Modification -</b> Unauthorized add, change, or delete of list data may have adverse ramifications that affect data integrity.  <b>Disruption -</b> Images and indices not available for period of time.	<ul style="list-style-type: none"> <li>• Appoint a security officer to monitor and manage security.</li> </ul>

Figure 3.1: Summary of Risk Assessment Results



### **3.3. Risk Considerations for Alternate Solutions**

Using the recommended safeguards contained in Figure 3.1: Summary of Risk Assessment Results, future needs were identified and included in Exhibit 2, *Needs Statement*. These future needs may have significant impact on the internal controls and security environment of any new system. These needs are:

- Provide for a network centric platform for FD and LDA system and maintain hardware, software, and data within the Clerk office.
- Ability to use Internet technologies for document distribution, potential public disclosure, and allow electronic filing and signature verification.

The impact of these needs on the internal controls and security environment is described below.

#### **3.3.1 Network Centric Platform**

The need for a network centric platform, which is located and operated entirely within the Clerk office, increases the Clerk's responsibility and accountability. HIR has physical and logical controls that provide reasonable protection from vulnerabilities. When evaluating the system alternatives, the Clerk should consider adopting the equivalent security standards as those implemented by HIR.

#### **3.3.2 Electronic Filing and Digital Signature**

Implementing electronic filing and digital signature functionality adds complexity to the management of the internal controls and security environment. Enabling electronic filing capabilities, with the need to verify signature, introduces new needs to protect the confidentiality, integrity, availability, and authentication of the data for filers. However, these security needs are addressed through specific technologies that are discussed below.

- **Confidentiality and Integrity.** Data encryption may be used to protect data during transmission of forms from either a Web site or e-mail source.
- **Authentication.** Electronic signature provides assurance that the file is truly from the sender. This provides non-repudiation (e.g., the filer cannot deny sending the file).
- **Availability.** Postal mail is continuously available. Electronic filing must be consistently available, particularly during the filing time window. Denial of service is a risk of electronic filing, and additional controls to address this risk would be needed.

**Exhibit 4**

**Exhibit 4**

**Feasibility Study**



**Feasibility Study**

**Table of Contents**

4.1. Methodology..... 1

    4.1.1 Analyze Needs and Define Evaluation Criteria..... 1

        4.1.1.1 Needs-Based Criteria ..... 1

        4.1.1.2 Assumptions and Constraints ..... 2

    4.1.2 Identify and Assess Range of Potential Alternatives..... 3

        4.1.2.1 Identification of Alternatives ..... 3

        4.1.2.2 Analysis of Potential Alternatives ..... 4

    4.1.3 Select and Develop Feasible Alternatives..... 6

4.2. Overview of Existing System ..... 6

    4.2.1 Stakeholder Analysis ..... 7

    4.2.2 Technology Description ..... 9

4.3. Alternative Systems ..... 10

    4.3.1 Alternative 1: Imaging/Workflow System..... 10

        4.3.1.1 Stakeholder Analysis..... 11

        4.3.1.2 Technology Description ..... 13

        4.3.1.3 High-Level Business Needs Evaluation ..... 15

        4.3.1.4 Implementation Issues..... 16

    4.3.2 Alternative 2: Imaging/Workflow System, with Electronic Filing and Basic Encryption ..... 17

        4.3.2.1 Stakeholder Analysis..... 17

        4.3.2.2 Technology Description ..... 19

        4.3.2.3 High-Level Business Needs Evaluation ..... 22

        4.3.2.4 Implementation Issues..... 23

    4.3.3 Alternative 3: Imaging/Workflow System with Electronic Filing and an Outsourced PKI ..... 24

        4.3.3.1 Stakeholder Analysis..... 24

        4.3.3.2 Technology Description ..... 27

        4.3.3.3 High-Level Business Needs Evaluation ..... 30

        4.3.3.4 Implementation Issues..... 31

    4.3.4 Alternative 4: Imaging/Workflow System with Electronic Filing and an In-house PKI ..... 32

        4.3.4.1 Stakeholder Analysis..... 32

        4.3.4.2 Technology Description ..... 34

        4.3.4.3 High-Level Business Needs Evaluation ..... 37

        4.3.4.4 Implementation Issues..... 38



## **Feasibility Study**

This exhibit presents the feasibility study of the Financial Disclosure (FD) and Lobby Disclosure Act (LDA) applications is presented. The purpose of the feasibility study is to identify and analyze alternative system approaches to meet the needs identified in Exhibit 2, *Needs Statement* and Exhibit 3, *Risk Assessment*. This exhibit, in conjunction with the cost-benefit analysis document, will provide the Office of the Clerk (Clerk) adequate information to make decisions to analyze and evaluate alternative systems to satisfy mission needs.

### **4.1. Methodology**

The feasibility study was developed using the following steps:

- Analyze Needs and Define Evaluation Criteria.
- Identify Range of Potential Alternatives.
- Select and Develop System Alternatives.

Listed below is a description of processes followed in completing each step.

#### **Analyze Needs and Define Evaluation Criteria**

The needs and risks of both applications were analyzed using the findings detailed in Exhibit 2, *Needs Statement* and Exhibit 3, *Risk Assessment*. The needs and risks formed the basis of the evaluation criteria that viable application alternatives should meet in order to be considered for implementation. The evaluation criteria is composed of: needs-based criteria, and assumptions and constraints identified in our analysis.

##### **4.1.1.1 Needs-Based Criteria**

The eight areas of functionality listed in Figure 4.1: Needs-Based Criteria Summary denote the needs-based criteria that were used to evaluate the system alternatives.

<b>Criterion Capability</b>	<b>Description</b>
Input	Ability to minimize the amount of manual data entry during forms processing and database compilation.
Processing	Allow for the automation of processing tasks (i.e., reporting non-responses and image destruction).
Output	Allow for flexible printing capabilities.
Query	Provide for flexible record query and reporting capabilities for both public and administrative use.
Storage	Ability to store images in commonly used and available media.
Technology	Allow document imaging and/or electronic filing with signature capabilities via the Internet. The alternatives should also provide a network centric platform (client-server) that can be maintained within the confines of the Clerk's office.
Application Controls and Security	Ability to authenticate users of the system, to protect data during electronic filing, to provide restricted access to data within the system, and provide for system availability on a timely and consistent basis.
Data Integrity Control	Ability to provide integrity and control, as noted in the risk assessment.

Figure 4.1: Needs-Based Criteria Summary (**Note:** Refer to Exhibit 2, *Needs Statement* for detailed information.)

#### 4.1.1.2 Assumptions and Constraints

In addition to the needs-based criteria used for evaluation, assumptions and constraints were identified that should be considered when evaluating the system alternatives. The assumptions and constraints are:

- **Scalability.** Any potential alternative must be scalable to meet all needs. For the purposes of this evaluation, the FD and LDA applications were examined, but any potential system alternative must be scalable to meet the other business needs within the Clerk's domain or other areas of the U.S. House of Representatives (House).
- **Use of Commercial-off-the-Shelf Applications.** The House's *Information Systems Program Plan, Management Policy for Systems Development Life Cycle (SDLC)*, dated June 28, 1996, states the desire to move towards Commercial-Off-The-Shelf (COTS) applications. For this analysis, COTS applications include solutions that may require significant customization to the needs of the House using commercially available software and development tools.
- **Implementation Time Frame.** Plans are currently underway to allow for a migration of all mission critical applications from the House's mainframe operated by the House Information Resources' (HIR) by the third quarter of Calendar Year (CY) 1999. Any potential alternative to

- replace the current FD and LDA applications should consider that migration plan when planning for the procurement or the implementation process.
  - **Economies of Scale.** The alternatives should allow for economies of scale, such as implementing technology that supports both the FD and LDA applications.
  - **No Significant Changes to Existing Laws.** The alternatives should not require significant changes to the Ethics in Government Act or LDA.

#### **4.1.2 Identify and Assess Range of Potential Alternatives**

To determine the various system alternatives for replacing the current FD and LDA applications, numerous sources were contacted to aid in the selection and evaluation. The approach used to research, identify, and analyze potential system alternatives is also included.

##### **4.1.2.1 Identification of Alternatives**

Our approach to researching alternatives included:

- **Interviewed Subject Matter Experts.** Several subject matter experts familiar with imaging systems and electronic filing technologies were interviewed. Areas of emphasis included imaging system technologies (e.g., Optical Character Recognition (OCR), Intelligent Character Recognition (ICR), workflow) and relevant cryptographic technologies (i.e., digital signature, Secure Socket Layer (SSL), Public Key Infrastructure (PKI), electronic filing functionality).
- **Reviewed Technology Literature.** A variety of sources were used to research potential COTS software, such as industry trade journals, the Internet, and vendor and product databases. Faulkner, Gartner Group, and Forrester proprietary information databases were used for information pertinent to imaging and electronic filing technologies, and various Internet searches were also performed to gather vendor information.
- **Interviewed Stakeholders and Other Government/Legislative Bodies.** Stakeholder opinions and preferences were gathered through interviews with key stakeholders of the FD and LDA applications. Key stakeholders (i.e., Legislative Computer Services (LCS), Legislative Resource Center (LRC)) were interviewed for technology and functionality preferences, limitations of current technical environment, and information pertaining to the current FileNet imaging system. Interviews with other government/legislative bodies (i.e., U.S. Senate, Canadian Lobby Registration Branch) were performed to gather information about electronic filing methods and efficiencies associated with the implementation of similar systems.



- Contacted Vendors to Identify Feasible Technologies.** Interviews with potential vendors that develop and distribute software and technologies that could potentially address the high-level business needs of the FD and LDA applications were performed. Information collected included data associated with product performance and functionality metrics. The identity of the House or Clerk was not disclosed, nor were vendors provided with Clerk-specific information. This was done to preserve vendor independence for any potential procurement in the future.

**4.1.2.2 Analysis of Potential Alternatives**

Using the criteria, assumptions, and constraints identified, an analysis of the system alternatives for replacing the current FD and LDA applications was performed. The selection of system alternatives included the identification of potential alternatives for the FD and LDA applications and the assessment of the feasibility of the alternatives. As a result of the feasibility assessment, some alternatives were found to be not viable because their functionality is inconsistent with the identified FD and LDA needs and constraints.

Figure 4.2: Summary Assessment of Potential Alternatives presents a description of the system alternatives that were identified and the assessment of the viability of each alternative highlighting the primary ways the alternative meets or does not meet the criteria.

Alternative	Description	Assessment
Retain Existing FileNet/Mainframe Applications	Keep the applications on the current HIR mainframe and RS-6000 platform.	<b>Not Viable</b> primarily because the alternative does not meet the needs criteria as noted in Figure 4.1 Needs-Based Criteria Summary in the following areas: (1) does not utilize client-server COTS technology, (2) is functionally not scalable, and (3) does not maintain hardware, software, and data within the Clerk’s office.
<i>Re-Platform Mainframe Index Applications to RS-6000 OS/390</i>	The FD and LDA mainframe index applications could be re-platformed to an RS/6000 environment within the confines of the Clerk.	<b>Not Viable</b> primarily because the alternative does not meet the needs criteria in Figure 4.1 Needs-Based Criteria Summary in the following areas: (1) does not utilize client-server COTS technology, (2) is not functionally scalable. Also, the Clerk does not intend to build the skill base to operate a mainframe operating system.

*Figure 4.2: Summary Assessment of Potential Alternatives*

Alternative	Description	Assessment
Replace mainframe index application with client-server application	Replace the current mainframe index application with a new client-server index application that would reside within the confines of the Clerk's office.	<b>Not Viable</b> primarily because the alternative does not meet the needs criteria in Figure 4.1 Needs-Based Criteria Summary in the following areas: (1) does not utilize client-server COTS technology and (2) is functionally not scalable.
Client-Server imaging/workflow system, with advanced forms processing functionality	<i>Implementation of a new client-server, COTS imaging system with advanced functionality that provides improved controls and processing techniques. This system would reside within the confines of the Clerk's office.</i>	<b>Viable</b> because it partially meets the high-level business needs and utilizes client-server technology. Although this alternative does not have electronic filing capabilities, the system could be developed to allow for future use of electronic filing and therefore is considered viable because it could be implemented to be scalable to incorporate electronic filing.
Electronic filing functionality with basic encryption techniques	Electronically file FD and LDA forms through a browser-based Internet application with SSL encryption techniques and challenge/response functionality.	<b>Viable</b> because the alternative: (1) meets the high-level business needs, (2) utilizes client-server COTS technology, and (3) is functionally scalable.
Electronic filing functionality with an <b>outsourced</b> <sup>12</sup> PKI	Electronically file FD and LDA forms through a browser-based Internet application using an external vendor to administer a PKI environment to provide enhanced encryption and digital signature measures.	<b>Viable</b> because the alternative: (1) meets the high-level business needs, (2) utilizes client-server COTS technology, and (3) is functionally scalable.
Electronic filing functionality with an <b>in-house</b> PKI implementation	Electronically file FD and LDA forms through a browser-based Internet application and the implementation of PKI to provide enhanced encryption and digital signature measures.	<b>Viable</b> because the alternative: (1) meets the high-level business needs, (2) utilizes client-server COTS technology, and (3) is functionally scalable.
Outsource all aspects of FD and LDA applications	Outsource the FD and LDA applications to a vendor outside of the Clerk's domain.	<b>Not Viable</b> because the alternative does not meet the needs criteria as noted in Figure 4.1 Needs-Based Criteria Summary associated with maintaining hardware, software, and data within the Clerk's office. The Ethics in Government Act and the Lobby Disclosure Act mandates that the Clerk process FD and LDA submissions.

*Figure 4.2: Summary Assessment of Potential Alternatives (continued)*

<sup>12</sup> For purposes of this study, outsourcing refers to administration of a system outside the confines of the Office of the Clerk. This could include outsourcing services provided by an external vendor or another House office (i.e., HIR).

### 4.1.3 Select and Develop Feasible Alternatives

The viable alternatives were grouped into four specific alternatives that would serve as implementation scenarios for further evaluation. The rationale used to group the viable alternatives was to provide the Clerk with a range of viable alternatives to consider and an analysis of viable technologies. The four alternatives selected for further evaluation in this exhibit include:

- **Imaging/Workflow System** represents the implementation of a new, client-server based imaging system that includes advanced forms processing functionality (i.e., OCR/ICR, workflow technologies).
- **Imaging/Workflow System and Electronic Filing with Basic Encryption** represents the implementation of a new imaging system, and adds functionality that would allow browser-based submission of FD and LDA forms via the Internet. The alternative includes the use of SSL and challenge/response authentication measures.
- **Imaging/Workflow System and Electronic Filing with an Outsourced Public Key Infrastructure** represents the implementation of a new imaging system, and adds functionality that allows for browser-based submission of FD and LDA forms via the Internet. The alternative includes the use of PKI encryption technology administered by an external service provider.
- **Imaging/Workflow System and Electronic Filing with an In-house Public Key Infrastructure** represents the implementation of a new imaging system, and adds functionality that allows for browser-based submission of FD and LDA forms via the Internet. The alternative includes the use of PKI encryption technology administered in-house by the Clerk.

In this exhibit, high-level implementation scenarios were developed for the alternatives identified above to represent the potential changes to the Clerk's organization and technology infrastructure.

### 4.2. Overview of Existing System

In this section, an overview of the existing system for the FD and LDA applications used by the Clerk is provided. An overview of the primary stakeholders and a description of the technology infrastructure is also included. As discussed in Figure 4.2: Summary Assessment of Potential Alternatives, the existing system was not considered a viable alternative because it does not meet the identified needs of the Clerk.

## 4.2.1 Stakeholder Analysis

Figure 4.3: Overview of Stakeholders for Existing System presents an overview of the stakeholders of the FD and LDA applications. In the following discussion, each of the stakeholders and their primary relationship to the FD and LDA applications is described.

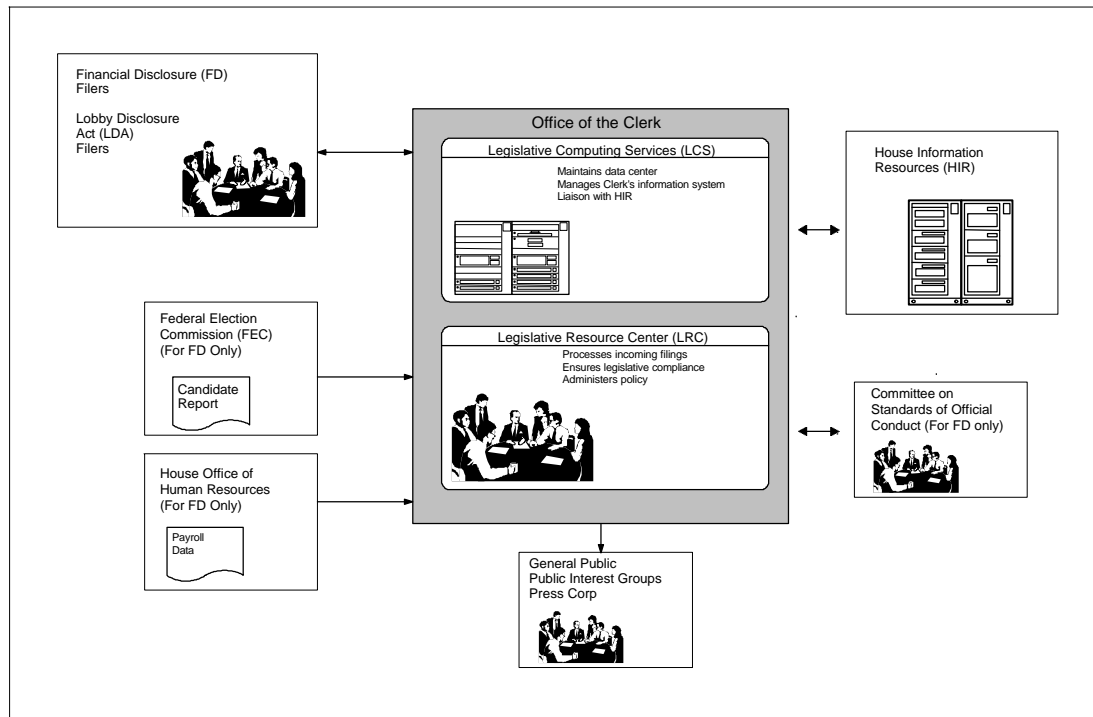


Figure 4.3: Overview of Stakeholders for Existing System

### Filing Community

- **Financial Disclosure Filers:** Members, Officers, certain employees, and candidates of the House manually submit FD Statements. The FD Statements are submitted on an annual basis. To date there are approximately 5,500 filers. Filers may download FD forms from the House Internet web site or may call the LRC directly to obtain the forms by mail. For the most recent processing year, the LRC received approximately 3,000 documents from the entire FD filing community.
- **Lobby Act Filers:** Individual lobbyists and lobbying firms manually register and file reports of their lobbying activities. The lobbying activity reports are manually submitted semi-annually no later than 45 days after the end of the first day of January and the first day of July. Filers call the LRC to request the LD-1 Form if they are new registrants or the LD-2 form if they are submitting their semi-annual report. These forms are also conveniently available on

- the Clerk's Internet web site in a downloadable format. There are currently a total of 3,727 active registrants who submit a total of 35,000 document pages per year.

### **Legislative Resource Center**

The LRC is the primary contact point for the House and handles incoming documents and fields telephone calls from the general public, public interest groups, the press corps, and FD and LDA filers. The LRC staff is comprised of a total of eight personnel who use the FD and LDA applications. Their primary functions are document scanning, indexing and quality control inspection and compliance processing.

Upon receipt of the registrant's documents via mail or dialup, LRC administrators scan and index the filings into the FileNet document management system. The scanning and processing of incoming documents involves extensive manual data input to enter index information and to properly track filing compliance.

### **Legislative Computer Systems**

The LCS has the responsibility for managing the information systems of the Clerk. The LCS maintains a data center in the Rayburn Building that houses the file servers and storage media for the FD and LDA applications. The LCS has one person assigned to provide overall technical support to the FD and LDA applications.<sup>13</sup>

### **House Information Resources**

The existing FD and LDA applications use the mainframe to store index information in an ADABAS database located on the HIR mainframe in the Ford Building. HIR personnel are responsible for maintenance for the image index application and are responsible for security administration for areas other than the FileNet system and the Clerk's local area network (LAN).

### **General Public**

Under the existing system, the LRC is the primary point of contact within the House. The general public, which includes public interest groups and the press corp, typically use workstations in the LRC facilities located in the Cannon Building to electronically view filer information.

---

<sup>13</sup> The Clerk indicated that this person spends approximately 40 percent of his time on supporting the FD and LDA applications.

## Federal Election Commission and Office of Human Resources

The Federal Election Commission (FEC) and the House's Office of Human Resources (OHR) submit information to the Clerk periodically, which is used by the LRC in processing the FD submissions. Information from the FEC and House OHR is provided in hard-copy report format, and the LRC uses this information to determine the expected filing community for the FD submissions.

## Committee on Standards of Official Conduct

After scanning the FD submissions into the FileNet system, the LRC forwards all FD forms to the Committee on Standards of Official Conduct for review. The LRC also forwards various ad hoc reports (i.e., non-respondent reports) regarding FD submissions to the Committee.

### 4.2.2 Technology Description

Figure 4.4: Overview of Existing System Technology Infrastructure presents an overview of the technology infrastructure associated with the existing system. The following discussion provides a high-level overview of the information technology components of the existing FD and LDA system.

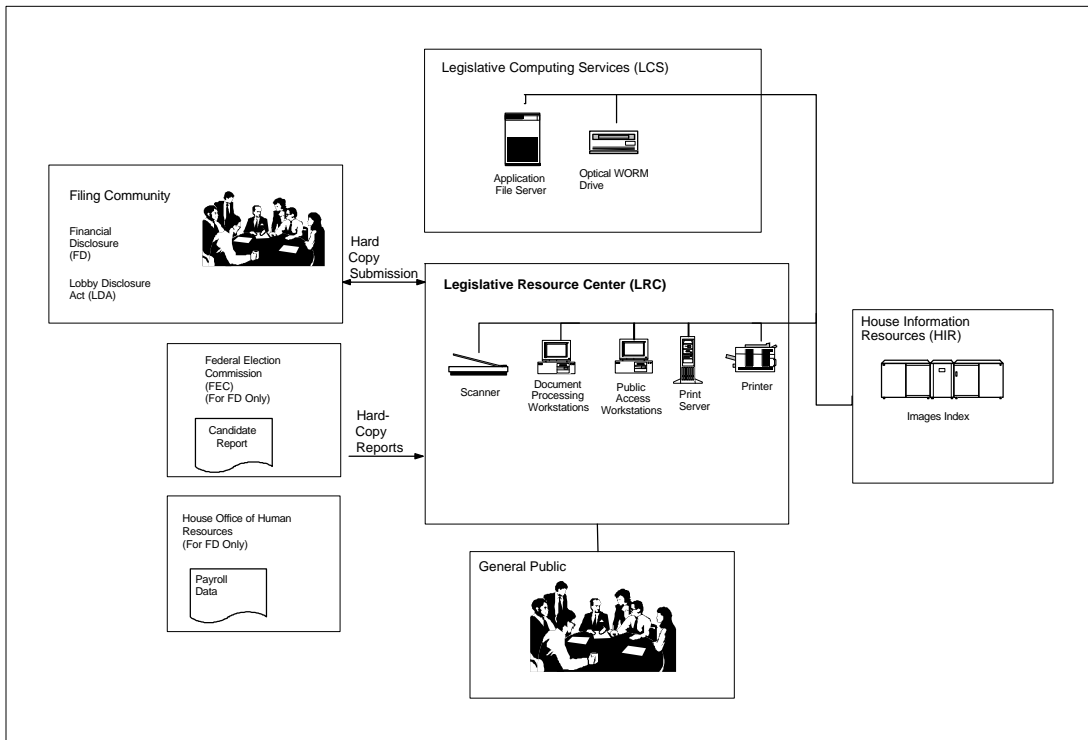


Figure 4.4: Overview of Existing System Technology Infrastructure

The primary components of the existing systems technology infrastructure are

- **Application File Server.** The FileNet application resides on two RS/6000 file servers using a UNIX operating system. The application is located in the LCS data center in the Rayburn Building. Print servers using OS/2 are housed in the LRC document process area.
- **Optical Image Storage.** Documents scanned and processed by FileNet are stored directly to a Write-One-Read-Many (WORM) optical platter. Images are stored in a standard TIFF format and may not be altered once they are written to disk. Currently, there is no mechanism for backing up the optical images.
- **Workstations.** There are two categories of workstations related to the FD and LDA applications. Workstations used by staff in the LCS for document scanning, indexing and routine data entry are appropriately equipped to handle the FileNet and mainframe terminal emulation clients. In addition, workstations are located in the public area of the LCS and are freely accessible for on-line document query.
- **Mainframe Images Index.** The FD and LDA indexes are maintained on an IBM Multiprise CMOS mainframe. LRC staff who process FD and LDA documents access the images index on the mainframe through a 3270 emulation client installed on their workstations. The mainframe is managed by HIR and is located in the Ford Building.

#### **4.3. Alternative Systems**

In this section, the viable alternatives to the existing system are presented, as noted in Figure 4.2: Summary Assessment of Potential Alternatives. The discussion of each alternative presents the following information:

- **Stakeholder Analysis** shows how the alternative would affect the primary FD and LDA stakeholders.
- **Technology Description** presents a high-level overview of the technology components, and relevant vendors, associated with the alternative.
- **High-Level Business Needs Evaluation** presents a summary of the evaluation of the alternative's ability to meet the high-level business needs as identified in Section D.1.1.1.
- **Implementation Issues** details any issues that need to be considered when evaluating the alternative.

##### **4.3.1 Alternative 1: Imaging/Workflow System**

In this section, the stakeholder analysis, technology description, high-level business needs evaluation, and implementation issues of the Imaging/Workflow System alternative are presented. The functionality of the Imaging/Workflow System alternative includes:

- **Imaging Application** that provides the functionality to maintain hard-copy submissions of FD and LDA forms in an optical format. The images maintained by the application are available for public view in the LCS.
- **Workflow Capabilities** that provide functionality for managing the processing of FD and LDA submissions in an automated fashion.
- **Optical Character Recognition/Intelligent Character Recognition** that provides the functionality to greatly reduce manual data entry of indexing information by providing the ability to optically recognize FD and LDA submission data as a form is being scanned into the imaging application.

As presented in Figure 4.2: Summary Assessment of Potential Alternatives, this alternative is viable because it partially meets the high-level business needs and utilizes client-server technology. Although this alternative does not have electronic filing capabilities, the system could be developed to allow for future use of electronic filing and therefore is considered viable because it could be implemented to be scalable to incorporate electronic filing.

#### **4.3.1.1 Stakeholder Analysis**

Figure 4.5: Alternative 1: Stakeholder Overview presents an overview of the stakeholders of the FD and LDA applications. In the discussion, each of the stakeholders and their primary relationship to the FD and LDA applications is described.



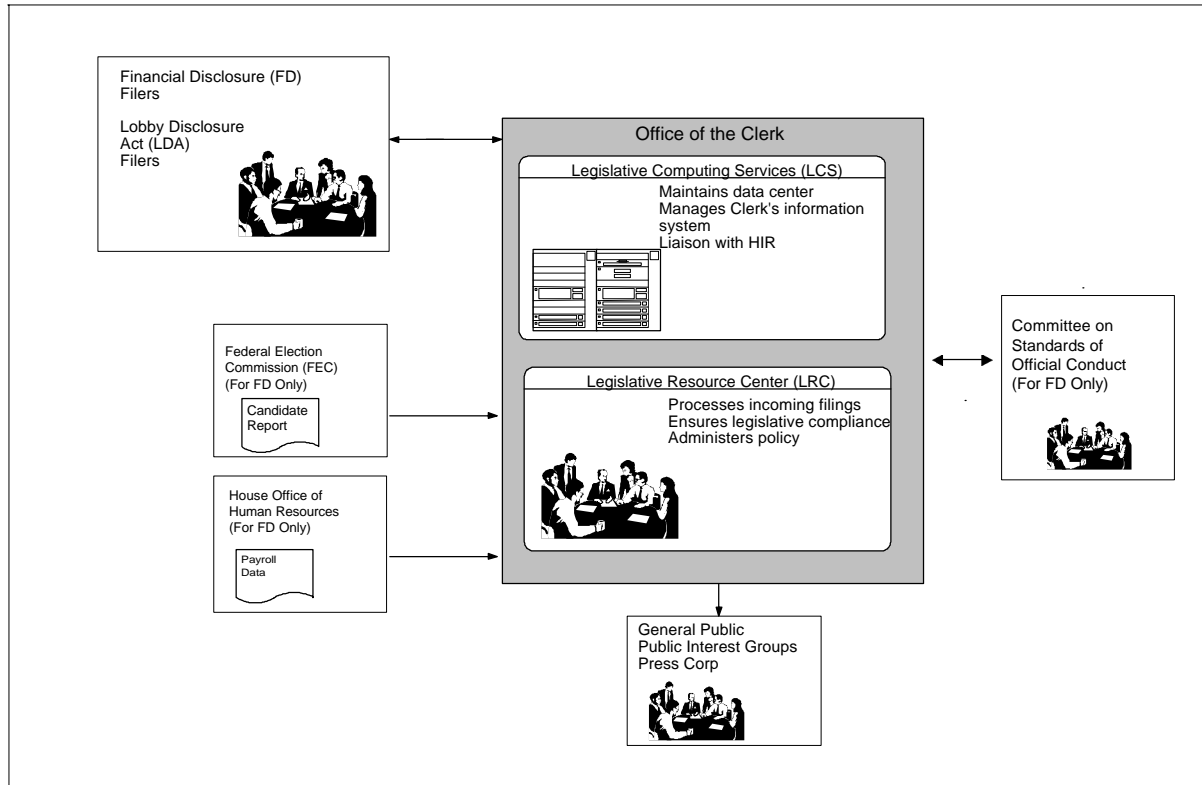


Figure 4.5: Alternative 1: Stakeholder Overview

## Filing Community

For this alternative, the filing community for the FD and LDA applications is largely unaffected in the manner in which they interact with the Clerk. Under this scenario, hard-copy forms continue to be submitted by mail and in-person and are subsequently processed by the LRC.

## Legislative Computer Systems

The migration of the FD and LDA indexes off of the HIR mainframe shifts the custody and management of all remaining hardware and software components to the LCS. Under this scenario, the LCS would need to assume greater responsibilities in the areas of security and data center management. The LCS would also be required to support the new imaging/workflow application and coordinate application maintenance with the chosen software vendor.

## Legislative Resource Center

Under this alternative, the relationship the LRC has with other stakeholders would remain essentially the same. However, it is likely the LRC would experience changes to their business processes as a

result of using a new imaging application with workflow and OCR/ICR capabilities. These changes to business processes would likely result in efficiencies in the processing function of the FD and LDA applications.<sup>14</sup>

### **House Information Resources**

All information systems processing and custody responsibilities for the index databases currently under the management of HIR would be eliminated.

### **General Public**

The general public is unaffected by this alternative in that they would continue to obtain FD and LDA information in person at the LRC or in printed format from GPO.

### **Federal Election Commission and Office of Human Resources**

This alternative would require cooperation from the FEC and the House's OHR in the development of an automated interface with the FD application to replace the existing manual interfaces. Automated interfaces would help improve the data integrity and the accuracy of incoming candidate and payroll information. Currently, the LRC staff receives hard-copy reports from the FEC and OHR that denote the expected filing community for the FD submissions. This automated interface would alleviate the need for manual data entry by providing a technical mechanism where the data from the FEC or OHR could be uploaded to the FD database with little or no manual intervention.

### **Committee on Standards of Official Conduct**

After scanning the FD submissions into the new system, the LRC would continue to forward all FD forms to the Committee on Standards of Official Conduct for review. The LRC would also continue to forward various ad hoc reports (i.e., non-respondent reports) regarding FD submissions to the Committee.

#### **4.3.1.2 Technology Description**

Figure 4.6: Alternative 1: Technology Overview presents an overview of the technology infrastructure associated with this alternative. The discussion following provides a high-level overview of the information technology components.

---

<sup>14</sup> Based on industry estimates for efficiencies achieved due to implementation of OCR/ICR and workflow technologies, we used the assumption that the current processing of hard copy FD and LDA submission could be performed using 20 percent less staff resources.

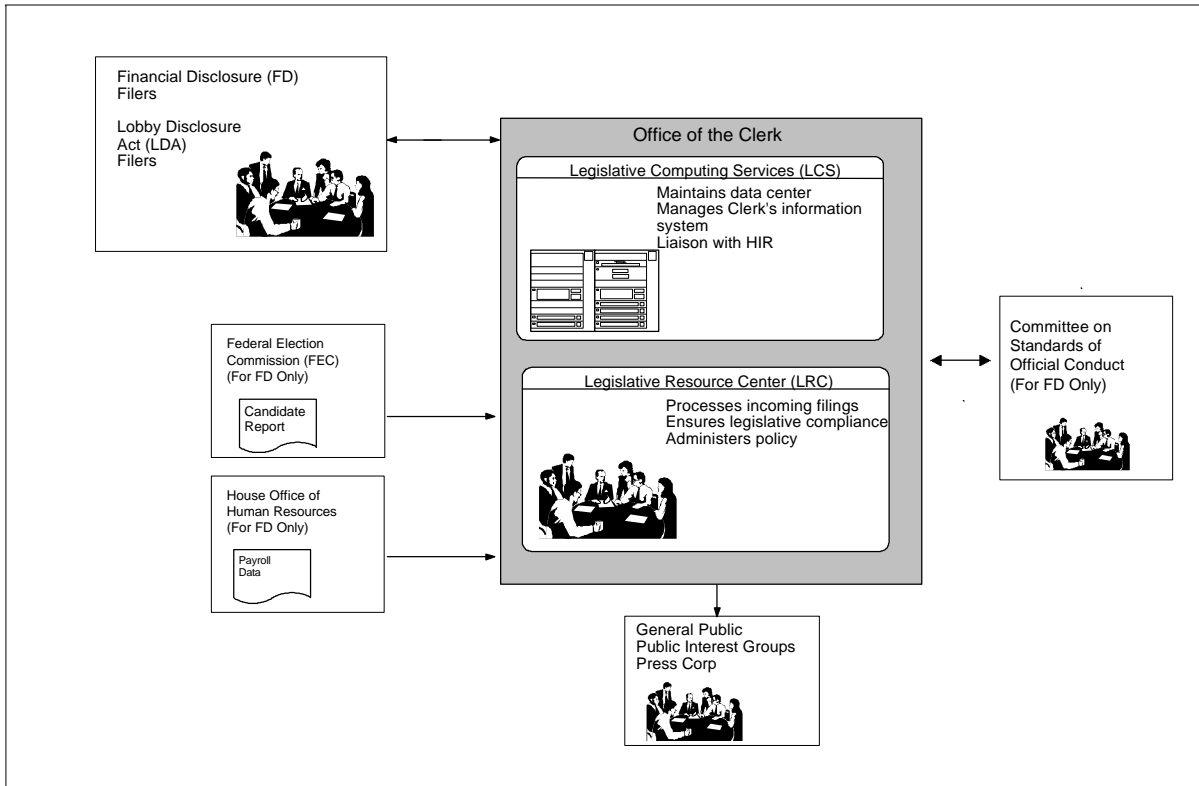


Figure 4.6: Alternative 1: Technology Overview

The primary components of this alternative's technology infrastructure are:

- **Imaging/Workflow Application.** The imaging application is the engine that drives the scanning, indexing and report writing process. It executes the core functions of any document management system in an integrated manner. Most significant of the possible improvements to the core document imaging functionality is the workflow management and OCR/ICR features. Workflow functions manage the flow of documents among administrators to ensure both accountability and quality assurance in the processing of information. Ideally, the application and the associated database engine should reside on separate servers for performance considerations. Modules added to the core application could provide a standardized (open) interface to minimize the amount of customized Application Program Interface (API) development necessary.
- **Storage Media and Backup.** Given the age and reliability of the Clerk's existing WORM drive, an upgrade to newer WORM technology should occur. A typical WORM 5.25-inch optical disk<sup>15</sup> holds up to 4.6G bytes of information, the equivalent of about one million

<sup>15</sup> Optical disk is the preferred media based on the issue of authenticating documents stored with digital media.

- pages or over 1800 standard 3.5-inch diskettes. The use of a digital-linear tape system used for backing up images from the WORM storage system should also be considered, at a minimum.
- **Scanning and Printing Peripherals.** To plan for future processing workloads, it may be necessary to upgrade the scanner and printing peripherals. The Clerk has made progress in this area by procuring high speed Xerox Docutech printers capable of on-demand printing. This should reduce the Clerk's reliance on the GPO for specific publicly disseminated reports.
- **Federal Election Commission and Office of Human Resources Interfaces.** The automation of data that has been previously entered by hand is critical to improving data integrity and accuracy. Telecommunication links could be established with the FEC and the OHR to allow for the timely upload of candidate and payroll data into the FD application. Although a high-speed telecommunication link is preferable, loading the information via tape could also be a viable alternative.

This alternative eliminates the need for the mainframe platform by shifting the image index database to a client-server architecture. The client-server model allows for specialized servers to distribute processing workloads. For example, separate file servers could handle such tasks as image processing, indexing, and printing. To maintain the functionality now processed on the mainframe component of the FD and LDA applications, it is likely that significant application customization to a COTS product would be needed to tailor the functionality to the specific needs of the FD and LDA system.

#### **4.3.1.3 High-Level Business Needs Evaluation**

This alternative was evaluated based on its ability to meet the high-level business needs as presented in Section 1.1.1 Needs Based Criteria. Figure 4.7: Alternative 1: Evaluation of High-Level Business Needs presents a summary of the evaluation of the high-level business needs.

Criteria	Criteria Rating	Assessment
Input Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• <i>This alternative reduces the inefficiencies and errors associated with data input. Automated interfaces for files received from the FEC and the OHR would eliminate the need for manual keying of hard copy reports.</i></li> <li>• OCR/ICR functionality speeds the input and creation of document index information.</li> </ul>
Processing Capabilities	<b>Partially</b>	<ul style="list-style-type: none"> <li>• Workflow functionality would improve quality assurance by providing the mechanism to administer controls associated with the FD and LDA processing cycle.</li> <li>• The core imaging system would incorporate logic to automate filer compliance.</li> </ul>
Output Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Standard report writing would be a component of the core imaging system.</li> <li>• The Xerox Docutech printer would be supported and allow for on-demand printing.</li> </ul>
Query Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Core system would include flexible, easy to use record query capabilities.</li> </ul>
Storage Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Image storage would be in a non-proprietary format.</li> </ul>
Technology Capabilities	<b>Partially</b>	<ul style="list-style-type: none"> <li>• The alternative does not include web-based file submission.</li> <li>• The alternative does not provide for potential public disclosure via the Internet.</li> <li>• Platform is network-centric in keeping with the House's desire to migrate from HIR's mainframe.</li> </ul>
Application Controls and Security Capabilities	<b>Partially</b>	<ul style="list-style-type: none"> <li>• The alternative does not provide web-based file submission, and thus the ability to protect data during electronic filing is not available.</li> <li>• Issues of authentication, confidentiality and data integrity are addressed in the core system functionality.</li> </ul>
Data Integrity Control Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Data integrity controls are improved through the use of workflow functionality and automated interfaces.</li> <li>• Field edits and error checking logic would be enhanced for all alternatives under consideration.</li> </ul>
<p>Key: <b>Partially</b>-Partially meets criteria <b>Fully</b>-Fully meets criteria</p>		

*Figure 4.7: Alternative 1: Evaluation of High-Level Business Needs*

#### **4.3.1.4 Implementation Issues**

The following implementation issues should be considered for this alternative:

- **Increased Information System Management Responsibility.** As a consequence of shifting portions of the FD and LDA process from HIR, the LCS would need to increase the scale of their security operations and data center management. Access to the imaging and database servers would need to be controlled both physically and logically. Additionally, administration workload would increase with the demands of supporting a larger production environment.
- **Impact of Workflow and OCR/ICR technology on LRC Business Processes.** Careful consideration would need to be given to the reengineering of the LRC's processes to accommodate workflow and OCR/ICR features of the new system.
- **Coordination Needed for Interface Development.** To develop automated interfaces with FEC and OHR systems, coordination with these organizations would be needed.

#### 4.3.2 Alternative 2: Imaging/Workflow System, with Electronic Filing and Basic Encryption

In this section, the stakeholder analysis, technology description, high-level business needs evaluation, and implementation issues of the Imaging/Workflow System, with Electronic Filing and Basic Encryption alternative are presented. The functionality of the Imaging/Workflow System with Electronic Filing and Basic Encryption alternative includes:

- **Imaging/Workflow System** that was described in the Imaging/Workflow alternative presented in Section 4.3.1, Alternative 1: Imaging/Workflow System.
- **Electronic Filing with Basic Encryption** that provides the functionality for electronic filing using basic encryption techniques and challenge/response security mechanisms. Electronic filing provides the FD and LDA user community the ability to file via the Internet using a user ID and password.

As presented in Figure 4.2: Summary Assessment of Potential Alternatives, this alternative meets the high-level business needs, constraints, and assumptions, including the criteria for electronic filing. However, it does not resolve the issue of non-repudiation. The alternative was still considered viable because the system could be developed so that it is scalable for future implementation of technology that addresses non-repudiation.<sup>16</sup>

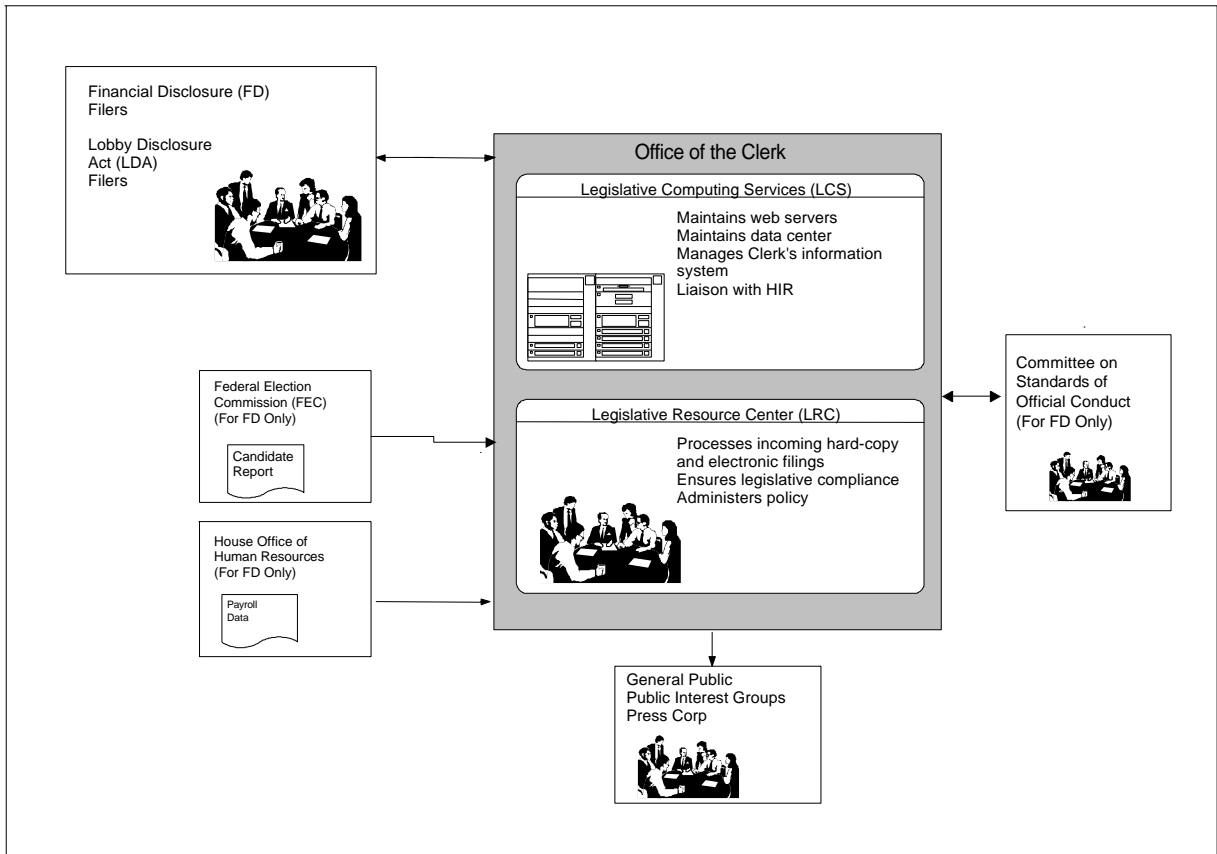
##### 4.3.2.1 Stakeholder Analysis

Figure 4.8: Alternative 2: Stakeholder Overview presents an overview of the primary stakeholders of the FD and LDA applications and their relationships. In the following discussion, each of the

---

<sup>16</sup> The alternative presented in Section 4.3.3, Imaging/Workflow System with Electronic Filing and an Outsourced PKI and Section 4.3.4, Imaging/Workflow System with Electronic Filing and an In-house PKI both address the non-repudiation issue. Non-repudiation refers to the ability of a filer to deny that he or she actually signed or sent a document to the Clerk.

stakeholders and their primary relationship to the FD and LDA applications under this alternative are described.



Figure

re 4.8: Alternative 2: Stakeholder Overview

### Legislative Computer Service

LCS would be responsible for managing and maintaining all of the technology components associated with the data center and Clerk information system components. Specifically, the LCS would now maintain the Internet technology components associated with the electronic filing functionality.

### Legislative Resource Center

The advent of electronic filing functionality would not preclude filers from submitting FD and LDA forms in hard copy format. The LRC would now be responsible for processing both hard copy and electronic submissions of FD and LDA information. FD and LDA data received via the Internet would be routed to the LRC for processing. The LRC processing staff would use the character-based data instead of the image of the hardcopy form to perform various edit checks and indexing processes

. This change would presumably lead to processing efficiencies, but the extent of these efficiencies is unclear.<sup>17</sup> The potential efficiencies that could be achieved with electronic filing are presented in Exhibit 5, *Cost-Benefit Analysis*, Section 5.3 Cost Sensitivity Analysis. The LRC would continue to ensure legislative compliance and administer policies associated with the FD and LDA laws.

### **FD and LDA Filing Community**

Filers of the FD and LDA forms would now have the ability to submit FD and LDA forms electronically via the Internet. The filer could connect to the Clerk's web site through a local Internet service provider and standard web browser or through the House intranet (for Members and House employees only) to submit their FD and LDA information for processing.

### **General Public**

The general public would still have access to all FD and LDA information submitted to the Clerk through the LRC. Hardcopy filings would be viewed as an image of the actual form (with signature) and electronic submissions would be viewed as the submitted data superimposed on an image of a blank form.

### **Federal Election Commission and Office of Human Resources**

This alternative would require cooperation from the FEC and the House's OHR in the development of automated interfaces with the FD application to replace the existing manual interface. Automated interfaces would help improve the data integrity and the accuracy of incoming candidate and payroll information.

### **Committee on Standards of Official Conduct**

After receiving the FD submissions, the LRC would continue to forward all FD forms to the Committee on Standards of Official Conduct for review. The LRC would also continue to forward various adhoc reports (i.e., non-respondent reports) regarding FD submissions to the Committee.

#### **4.3.2.2 Technology Description**

Figure 4.9: Alternative 2: Technology Description presents an overview of the technology infrastructure associated with this alternative. The following discussion provides a high-level overview of the information technology components.

---

<sup>17</sup> Although the implementation of electronic filing technology would be expected to generate efficiencies from reduced data entry of hard copy forms, the specific amount of labor cost savings is unclear. Therefore, we have not made any assumptions with regard to labor cost efficiencies from electronic filing.



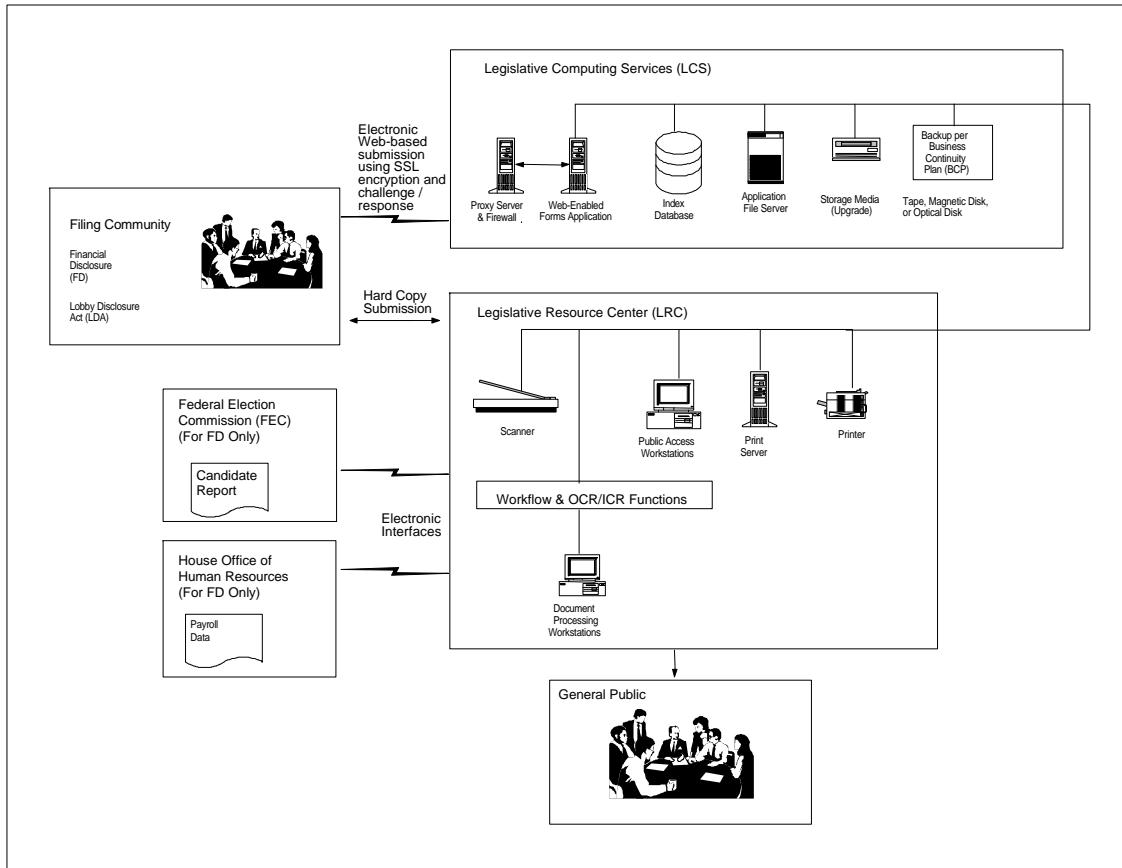


Figure 4.9: Alternative 2: Technology Description

### Imaging/Workflow System Components

This alternative includes the technology components indicated in the previous alternative described in Section 3.1, Alternative 1: Imaging/Workflow System. Those technology components are summarized as followed:

- Imaging/Workflow Application.** The imaging application is the engine that drives the scanning, indexing and report writing process. Most significant of the possible improvements to the core document imaging functionality is the workflow management and OCR/ICR features. Workflow functions manage the flow of documents among administrators to ensure both accountability and quality assurance in the processing of information.

- **Storage Media and Backup.** Given the age and unreliable state of the existing WORM drive, upgrading to newer WORM technology and implementing a digital-linear tape backup system should be considered, at a minimum.
- **Scanning and Printing Peripherals.** To plan for future processing loads, it may be necessary to upgrade the scanner and printing peripherals. The Clerk has made progress in this area by procuring high speed Xerox Docutech printers capable of on-demand printing. This should reduce the Clerk's reliance on the GPO for specific publicly disseminated reports.
- **Federal Election Commission and Office of Human Resources Interfaces.** The automation of data that has been previously entered by hand is critical to improving data integrity and accuracy. Telecommunication links could be established with the FEC and the OHR to allow for the timely upload of candidate and payroll data into the FD application. Although a high-speed telecommunication link is preferable, loading the information via tape could also be a viable alternative.

### Electronic Filing Components

Providing an environment for electronic filing requires that various technology components be employed. The use of secure Internet web servers for this purpose is a widely used and accepted practice. A web-based forms application that uses SSL encryption and challenge/response (user ID and password) measures to provide basic levels of confidentiality, data integrity, and authentication is also a widely used method for capturing information via the Internet. Although there are many benefits that can be achieved by allowing electronic submission of the FD and LDA forms, electronic submission of information introduces many vulnerabilities and security risks such as public viewing of FD or LDA information before the LRC staff processing cycle is completed.

Technology components that address this security are:

- **Web-based Forms Application.** A web-based forms application would be developed that would allow filers to dynamically fill out their FD and LDA forms. The web pages would resemble the actual paper forms, and would capture all the information normally submitted on the hardcopy documents. These web-based forms could employ inherent intelligence that performs routine edit checks while the respondent inputs data. If the respondent somehow fills out a cell with incorrect information (i.e., enters a wrong date or invalid state code) the web application could be enabled to reject the submission and guide the respondent to a correct/acceptable response. After submitting the forms, the data could be automatically indexed and stored based on the information provided by the respondent.
- **Web Server Hardware/Software (SSL).** The web-based forms application detailed above would physically reside on a Internet web server within the confines of the LCS. This web server would

- have the capability to support encrypted connections initiated by the web clients (i.e., FD and LDA submission population) and through use of a SSL connection. SSL functions in a paired environment, where a secure client (e.g., FD or LDA submitter) connects with a secure server. SSL uses public encryption technology that would render the FD and LDA submissions routable but unreadable by intermediate hosts. The SSL technology authenticates servers, preventing an intermediate interception of data on the network from others posing as the destination server (in this case, the House). This method of encryption protects Internet communications and ensures data integrity associated with electronic submissions. SSL is used by developers to add security within TCP/IP applications and has become a de facto standard for encryption between browsers and servers.
- **Challenge/Response Mechanism.** Access to the FD and LDA web-based applications would be granted through a password and account ID mechanism. This challenge/response mechanism would authenticate users who choose to submit FD and LDA forms via the Internet. Included with this alternative is the necessity to issue user IDs/passwords to filers in some way, prior to being granted access to the system (i.e., mail, email, in person). SSL combined with account ID and passwords would provide the basic levels of confidentiality, integrity, and authentication needed to support FD and LDA electronic submission.
- **Proxy Server and Firewall.** A proxy server and firewall are required to protect the web server and web-based forms application from unauthorized uses such as those wishing to infiltrate and disrupt the system.

#### **4.3.2.3 High-Level Business Needs Evaluation**

This alternative was evaluated based on the evaluation criteria derived from the high-level business needs, constraints, and assumptions. Figure 4.10: Alternative 2: Evaluation of High-Level Business Needs presents a summary assessment of the how this alternative satisfies the business needs.

Criteria	Criteria Rating	Assessment
Input Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• <i>This alternative reduces the inefficiencies and errors associated with data input. Automated interfaces for files received from the FEC and OHR would eliminate the need for manual keying of hard copy reports.</i></li> <li>• OCR/ICR functionality speeds the input of document index information.</li> </ul>
Processing Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Workflow functionality would improve quality assurance by providing the mechanism to administer controls associated with the FD and LDA processing cycle.</li> <li>• The core imaging system would incorporate logic to automate filer compliance.</li> </ul>
Output Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Standard report writing would be a component of the core imaging system.</li> <li>• The Xerox Docutech printer would be supported and allow for on-demand printing.</li> </ul>
Query Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Core system would include flexible, easy to use record query capabilities.</li> </ul>
Storage Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Image storage would be in a non-proprietary format.</li> </ul>
Technology Capabilities	<b>Partially</b>	<ul style="list-style-type: none"> <li>• This alternative does provide functionality that allows for electronic filing of FD and LDA submissions, but does not provide the non-repudiation of submissions.</li> </ul>
Application Controls and Security Capabilities	<b>Partially</b>	<ul style="list-style-type: none"> <li>• This alternative does provide basic protection of data during electronic submission by use of SSL encryption, but does not provide for non-repudiation.</li> </ul>
Data Integrity Control Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Data integrity controls are improved through the use of workflow functionality and automated interfaces.</li> <li>• Field edits and error checking logic would be enhanced for all alternatives under consideration.</li> </ul>
Key: <b>Partially</b> -Partially meets criteria <b>Fully</b> -Fully meets criteria		

*Figure 4.10: Alternative 2: Evaluation of High-Level Business Needs*

#### **4.3.2.4 Implementation Issues**

There are a number of implementation issues that need to be considered when evaluating whether to use electronic filing of FD and LDA submissions with the use of basic encryption and challenge/response security techniques. The primary implementation issues are:

- **Non-Repudiation.**<sup>18</sup> The legal issues surrounding the use of electronic filing of FD and LDA submissions involve non-repudiation and the acceptability of digital information in a court of law.
- Research should be undertaken to derive conclusions of the appropriateness of using electronic filing prior to investment in this technology.
- **Acceptance of Electronic Filing by the User Community.** The use and acceptance of electronic filing by FD and LDA filers is currently unclear. In Canada, approximately 95 percent of lobbyists submit information electronically. However, the Canadian Government assesses significant user fees to lobbyists who submit paper forms. Although Internet technologies have gained wide acceptance within the U.S., it is unclear to what extent FD and LDA filers would file using electronic methods. The Clerk should, at a minimum, survey FD and LDA filers to gauge acceptance and usage prior to investing in electronic filing technologies.

#### 4.3.3 Alternative 3: Imaging/Workflow System with Electronic Filing and an Outsourced PKI

In this section, the stakeholder analysis, technology description, high-level business needs evaluation, and implementation issues of the Imaging/Workflow System, with Electronic Filing and an outsourced PKI alternative are presented. The functionality of the Imaging/Workflow System with Electronic Filing and an Outsourced PKI system alternative includes:

- **Imaging/Workflow System** that was described in the Imaging/Workflow alternative presented in Section 4.3.1, Alternative 1: Imaging/Workflow System.
- **Electronic Filing** that provides the functionality for electronic filing. Electronic filing provides the FD and LDA user community the ability to file via the Internet using a user ID and password that was described in the alternative described in Section 4.3.2, Alternative 2: Imaging/Workflow System with Electronic Filing with Basic Encryption.
- **Public Key Infrastructure** that provides the functionality for electronic filing with the use of a PKI. The implementation of PKI could provide increased levels of confidentiality, integrity, and authentication of electronic submissions of FD and LDA forms and could address the non-repudiation evaluation criterion. For this alternative, the PKI system would be administered by a PKI outsourcing agent.

This alternative meets the evaluation criteria, including the electronic filing functionality. The alternative provides added features in the areas of security and non-repudiation through the use of a PKI. However, it does present issues with regard to management control of the entire PKI process.

##### 4.3.3.1 Stakeholder Analysis

Figure 4.11: Alternative 3: Stakeholder Overview presents an overview of the primary stakeholders of the FD and LDA applications and their relationships. In the following discussion, each of the

---

<sup>18</sup> Non-repudiation refers to the ability to validate whether a filer actually signed or sent a document to the Clerk.

stakeholders and their primary relationship to the FD and LDA applications under this alternative are described.

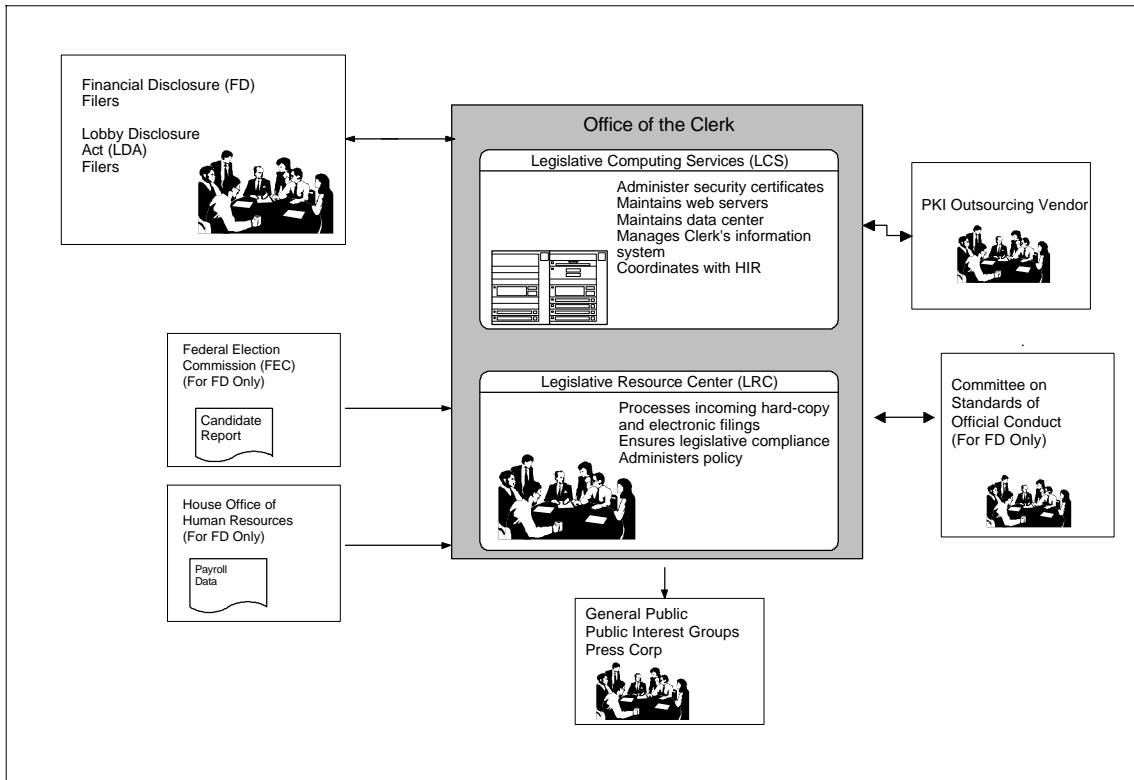


Figure 4.11: Alternative 3: Stakeholder Overview

### PKI Outsourcing Vendor

The PKI outsourcing vendor would serve as the management (i.e., storing, revoking, updating) of the electronic signatures that filers would use to authenticate submissions of the FD and LDA forms. The outsourcing agent would also be responsible for the distribution of these electronic signatures. The electronic submission would be done through the use of a House branded web site maintained and operated by the outsourcing agent.

### Filing Community

To sustain the integrity of the PKI environment, the FD and LDA filing community would face additional scrutiny with regards to proof of identification. Verifying the identity of users of a PKI is paramount to the security that the PKI provides. Filers would need to provide proof of identification before they would be allowed to submit electronically. Filers could provide proof of identity and sign an agreement for authorized use in person at the LRC. Another method could involve submitting a request through the mail by providing a notarized letter using official letterhead.

### **Legislative Computer Services**

The implementation of a PKI would require the LCS to develop an understanding and a competency of a number of additional technical areas. In addition to the basic Internet components associated with electronic filing detailed in Section 4.3.2, Imaging/Workflow System with Electronic Filing with Basic Encryption, the LCS would need to have an interface with the PKI outsourcing agent. This interface would serve as the means by which the Clerk notifies the outsourcing agent of new users of the system. The LCS would also be responsible for developing and deploying new policies and procedures that address sustaining a PKI environment.

### **Legislative Resource Center**

In addition to the duties of processing the hardcopy and electronic submissions of the FD and LDA forms, the LRC would also be involved in the development of policies and procedures associated with the management of the PKI environment. The LRC would also be involved with administering those policies and procedures within the FD and LDA user community.

### **General Public**

The general public would still have access to all FD and LDA information submitted to the Clerk through the LRC public access terminals. Hardcopy filings would be viewed as an image of the actual form (with signature) and electronic submissions would be viewed as the submitted data superimposed on an image of a blank form.

### **Federal Election Commission and Office of Human Resources**

This alternative would require cooperation from the FEC and the House's OHR in the development of automated interfaces with the FD application to replace the existing manual interfaces. Automated interfaces would help improve the data integrity and the accuracy of incoming candidate and payroll information.

### **Committee on Standards of Official Conduct**

After receiving the FD submissions, the LRC would continue to forward all FD forms to the Committee on Standards of Official Conduct for review. The LRC would also continue to forward various adhoc reports (i.e., non-respondent reports) regarding FD submissions to the Committee.

### 4.3.3.2 Technology Description

Figure 4.12: Alternative 3: Technology Overview presents an overview of the technology infrastructure associated with this alternative. The following discussion provides a high-level overview of the information technology components.

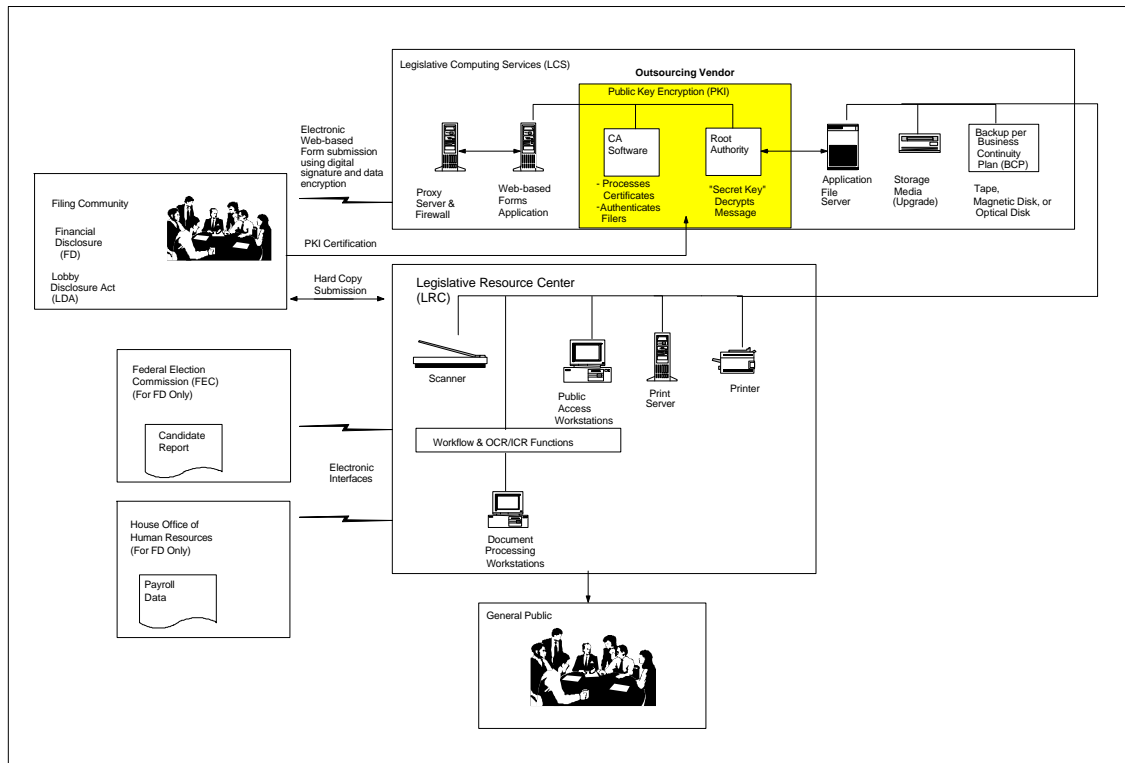


Figure 4.12: Alternative 3: Technology Overview

### Imaging/Workflow System Components

This alternative includes the technology components indicated in the previous alternative described in Section 3.1, Alternative 1: Imaging/Workflow System. Those technology components are summarized as followed:

- Imaging/Workflow Application.** The imaging application is the engine that drives the scanning, indexing and report writing process. It executes the core functions of any document management system in an integrated manner. Most significant of the possible improvements to the core document imaging functionality is the workflow management and OCR/ICR features. Workflow functions manage the flow of documents among administrators to ensure both accountability and quality assurance in the processing of information.



- **Storage Media and Backup.** Given the age and unreliable state of the existing WORM drive, upgrading to newer WORM technology implementing a digital-linear tape backup system should be considered, at a minimum.
- **Scanning and Printing Peripherals.** To plan for future processing loads, it may be necessary to upgrade the scanner and printing peripherals. The Clerk has made progress in this area by procuring high speed Xerox Docutech printers capable of on-demand printing. This should reduce the Clerk's reliance on the GPO for specific publicly disseminated reports.
- **Federal Election Commission and Office of Human Resources Interfaces.** The automation of data that has been previously entered by hand is critical to improving data integrity and accuracy. Telecommunication links could be established with the FEC and OHR to allow for the timely upload of candidate and payroll data into the FD application. Although a high-speed telecommunication link is preferable, loading the information via tape could also be a viable alternative.

### **Electronic Filing Components**

This alternative includes the technology components indicated in the previous alternative described in Section 3.2, Alternative 2: Imaging/Workflow System with Electronic Filing and Basic Encryption. Those technology components are summarized as followed:

- **Web-based Forms Application.** A web-based forms application would be developed that would allow filers to dynamically fill out their FD and LDA forms.
- **Web Server Hardware/Software (SSL).** The web-based forms application detailed above would physically reside on a Internet web server within the confines of the LCS. This web server would have the capability to support encrypted connections initiated by the web clients (i.e., FD and LDA submission population) and through the use of a SSL connection.
- **Challenge/Response Mechanism.** Access to the FD and LDA web-based applications would be granted through a password and account ID mechanism. This challenge/response mechanism would authenticate users who choose to submit FD and LDA forms via the Internet using user IDs and passwords.
- **Proxy Server and Firewall.** A proxy server and firewall are required to protect the web server and web-based forms application from unauthorized uses by those wishing to infiltrate and disrupt the system.

## Public Key Infrastructure Components

A PKI environment is implemented using a mix of hardware and software components, combined with related policies and procedures, to provide a set of security services that enable secure electronic computing in a distributed environment. The outsourcing agent would be responsible for the technology components of the PKI, and the Clerk would be responsible for developing and implementing the policies and procedures that govern the PKI.

To provide an electronic filing functionality with a PKI environment, the following technology components would need to be employed:

- **Certificates.** After providing proof of identification, a filer wishing to submit FD or LDA forms electronically in a PKI environment would receive a unique digital certificate (from the outsourcing agent, after receiving notification from the Clerk) that would be used to authenticate their submission. Certificates are the mechanism by which a person's identity associated with an electronic submission can be authenticated. These unique certificates serve as electronic signatures, thereby authenticating the identity of an electronic filer. The digital certificate could be physically stored as a plug-in to the sender's web browser that resides on their PC. This unique certificate, when provided with an electronic submission of the FD or LDA forms, would provide non-repudiation of identity of the filer.
- **Certificate Authority (CA).** The primary function of the CA is to generate and manage the public key certificates that bind the user's identity with the user's public key. In order to perform this function, a CA must provide various services<sup>19</sup> to the users of the certificates. Major services performed by a CA are detailed as follows:
  - *Certificate Generation:* One of the most important services provided by a CA is the generation of certificates. It is through certificate generation that the binding of a user's identity and a user's public key is made which, in turn, is based on the appropriate user identification methods.
  - *Certificate Authorization:* When a certificate is presented, the CA verifies that the certificate is valid and is authorized for the given use.
  - *Certificate Maintenance:* The CA must perform a number of maintenance activities associated with certificates. Common maintenance activities include certificate back-up and revocation.

---

<sup>19</sup> Depending upon the nature of the vendor service agreement, various functions can be shared by both the outsourcing provider and the Clerk.

The functions listed above are generally performed using a combination of CA software and accompanying CA policy and procedures. Some popular PKI vendors that perform this function include products such as Spryus/Signet CA, Entrust WebCA, and IBM Registry.

- **Directory Servers.** The directory server is responsible for maintaining the actual certificates and user identification pairs for future authentication purposes.
- **Root Authority (RA).** The RA is the single point of trust at the top of a certification hierarchy of a PKI.<sup>20</sup> What separates this CA from other CAs is that it signs its own certificate. Because of this, its private key must be highly protected. The RA usually issues certificates for subordinate CAs. A number of RAs are currently in use in the Internet. For example, Netscape offers RA certificates from 16 organizations including, but not limited to Verisign, GTE, and AT&T.

#### **4.3.3.3 High-Level Business Needs Evaluation**

This alternative was evaluated based on its ability to meet the high-level business needs as presented in Section 1.1.1 Needs Based Criteria. Figure 4.13: Alternative 3: Evaluation of High-Level Business Needs presents a summary of the evaluation of the high-level business needs.

---

<sup>20</sup> The RA is also referred to as a Top-Level Certification Authority (TLCA).

Criteria	Criteria Rating	Comment
Input Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• <i>This alternative reduces the inefficiencies and errors associated with data input. Automated interfaces for files received from the FEC and the OHR would eliminate the need for manual keying of hard copy reports.</i></li> <li>• OCR/ICR functionality speeds the input of document index information.</li> </ul>
Processing Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Workflow functionality would improve quality assurance by providing the mechanism to administer controls associated with the FD and LDA processing cycle.</li> <li>• The core imaging system would incorporate logic to automate filer compliance.</li> </ul>
Output Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Standard report writing would be a component of the core imaging system.</li> <li>• The Xerox Docutech printer would be supported and allow for on-demand printing.</li> </ul>
Query Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Core system would include flexible, easy to use record query capabilities.</li> </ul>
Storage Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Image storage would be in a non-proprietary format.</li> </ul>
Technology Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• This alternative provides enhanced capabilities for electronic filing and signature verification. Implementation of PKI provides non-repudiation of electronic FD and LDA submissions. This functionality is not included in the Imaging/Workflow System, with Electronic Filing and Basic Encryption alternative.</li> </ul>
Application Controls and Security Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• This alternative provides increased protection of data submitted electronically, along with non-repudiation assurances.</li> </ul>
Data Integrity Control Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Data integrity controls are improved through the use of workflow functionality and automated interfaces.</li> <li>• Field edits and error checking logic would be enhanced for all alternatives under consideration.</li> </ul>
<p>Key: <b>Partially</b>-Partially meets criteria    <b>Fully</b>-Fully meets criteria</p>		

*Figure 4.13: Alternative 3: Evaluation of High-Level Business Needs*

#### 4.3.3.4 Implementation Issues

There are number of implementation issues that need to be considered when evaluating whether to implement an outsourced PKI. The primary implementation issues are:

- **Clerk-Wide vs. House-Wide Implementation of PKI.** The model detailed above shows the PKI residing within the LRC, under the direction of the Clerk. This PKI model could serve as a pilot to assess its viability to other scenarios that fit within the mission of the entire House. For example, one use of the PKI technology's digital certificates involves the use of physical "smart cards". These cards can be designed to carry a physically embedded digital certificates that, when swiped through a card reader, provide a unique digital signature. Applications that would fit this model could include House Member vote casting, House employee parking validation or substantiation of a FD and LDA hardcopy submission.
- **Outsource Agent Issues.** The Clerk must be cognizant that the overall security of the environment would depend somewhat on the security practices of the outsourcing agent. The Clerk would have less control of the security aspect of this application.

#### 4.3.4 Alternative 4: Imaging/Workflow System with Electronic Filing and an In-house PKI

In this section, the stakeholder analysis, technology description, high-level business needs evaluation, and implementation issues of the Imaging/Workflow System, with Electronic Filing and an In-house PKI alternative are presented. The functionality of the Imaging/Workflow System with Electronic Filing and In-house PKI system alternative includes:

- **Imaging/Workflow System** that was described in the Imaging/Workflow alternative presented in Section 4.3.1, Alternative 1: Imaging/Workflow System.
- **Electronic Filing** that provides the functionality for electronic filing. Electronic filing provides the FD and LDA user community the ability to file via the Internet using a user ID and password that was described in the alternative described in Section 4.3.2, Alternative 2: Imaging/Workflow System with Electronic Filing and Basic Encryption.
- **Public Key Infrastructure** that provides the functionality for electronic filing with the use of a PKI. The implementation of PKI could provide increased levels of confidentiality, integrity, and authentication of electronic submissions of FD and LDA forms and could address the non-repudiation evaluation criterion. For this alternative, the PKI system would be administered in-house by the Clerk.

This alternative meets the evaluation criteria, including electronic filing. The alternative provides added features in the area of security and non-repudiation through the use of a PKI.

##### D.3.4.1 Stakeholder Analysis

Figure 4.14: Alternative 4: Stakeholder Overview presents an overview of the primary stakeholders of the FD and LDA applications and their relationships. In the following discussion, each of the

stakeholders and their primary relationship to the FD and LDA applications under this alternative are described.

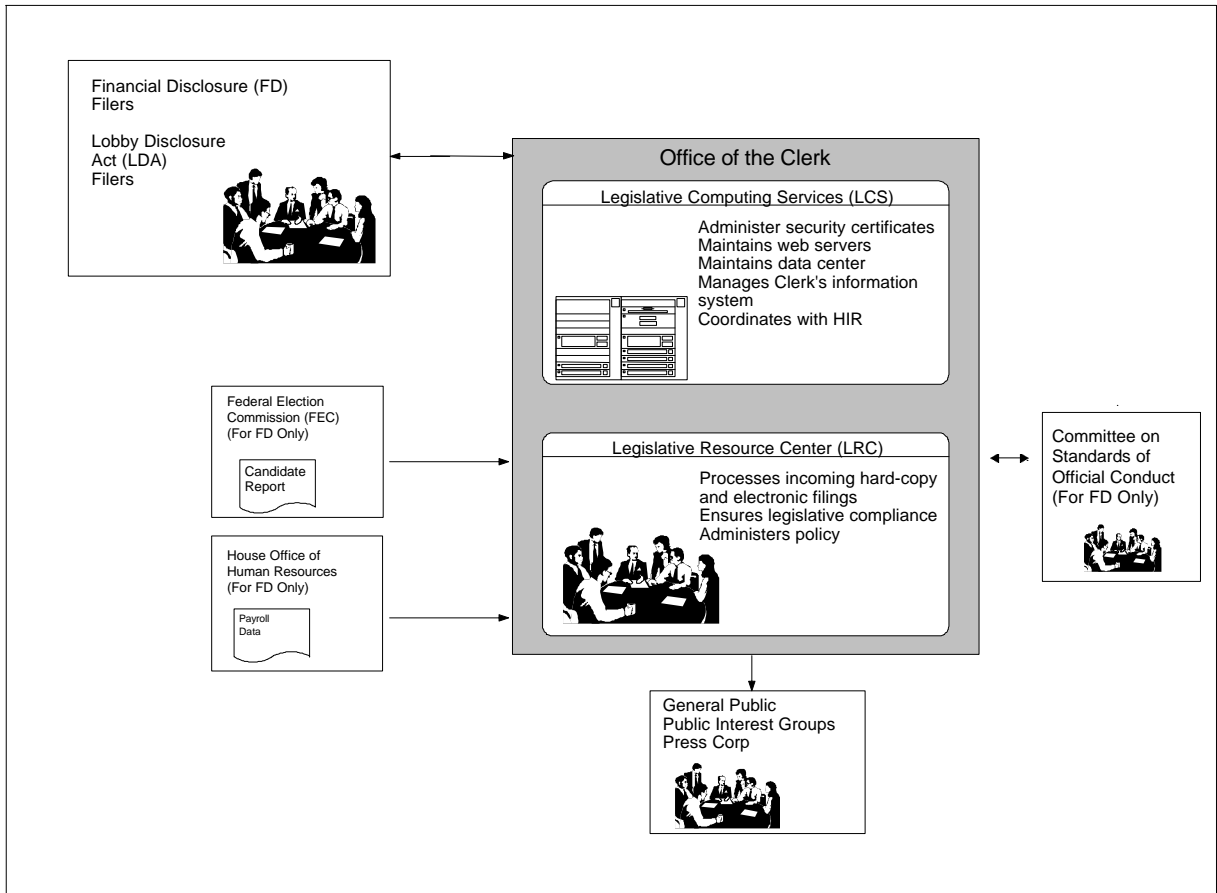


Figure 4.14: Alternative 4: Stakeholder Overview

### Filing Community

To sustain the integrity of the PKI environment, the FD and LDA filing community would face additional scrutiny with regards to proof of identification. Verifying the identity of users of a PKI is paramount to the health of the security that the PKI provides. Filers would need to provide proof of identification before they would be allowed to submit electronically. Filers could provide proof of identity and sign an agreement for authorized use in person at the LRC. Another method could involve submitting a request through the mail by providing a notarized letter using official letterhead.

### **Legislative Computer Services**

The implementation of a PKI would require the LCS to develop an understanding and a competency of a number of additional technical areas. In addition to the basic Internet components associated with electronic filing detailed in Section 4.3.2, Alternative 2: Imaging/Workflow System with Electronic Filing with Basic Encryption, the LCS would be responsible for the operation of the PKI and the technology components if operated in-house. The technology components include new software and hardware, as well as new policies and procedures that address sustaining a PKI environment.

### **Legislative Resource Center**

In addition to the duties of processing the hardcopy and electronic submissions of the FD and LDA forms, the LRC would also be involved in the development of policies and procedures associated with the management of the PKI environment. The LRC would also be involved with administering those policies and procedures within the FD and LDA user community.

### **General Public**

The general public would still have access to all FD and LDA information submitted to the Clerk through the LRC public access terminals. Hardcopy filings would be viewed as an image of the actual form (with signature) and electronic submissions would be viewed as the submitted data superimposed on an image of a blank form.

### **Federal Election Commission and Office of Human Resources**

This alternative would require cooperation from the FEC and the House's OHR in the development of automated interfaces with the FD application to replace the existing manual interface. Automated interfaces would help improve the data integrity and the accuracy of incoming candidate and payroll information.

### **Committee on Standards of Official Conduct**

After receiving the FD submissions, the LRC would continue to forward all FD forms to the Committee on Standards of Official Conduct for review. The LRC would also continue to forward various adhoc reports (i.e., non-respondent reports) regarding FD submissions to the Committee.

#### **4.3.4.2 Technology Description**

Figure 4.15: Alternative 4: Technology Overview presents an overview of the technology infrastructure associated with this alternative. The following discussion provides a high-level overview of the information technology components.

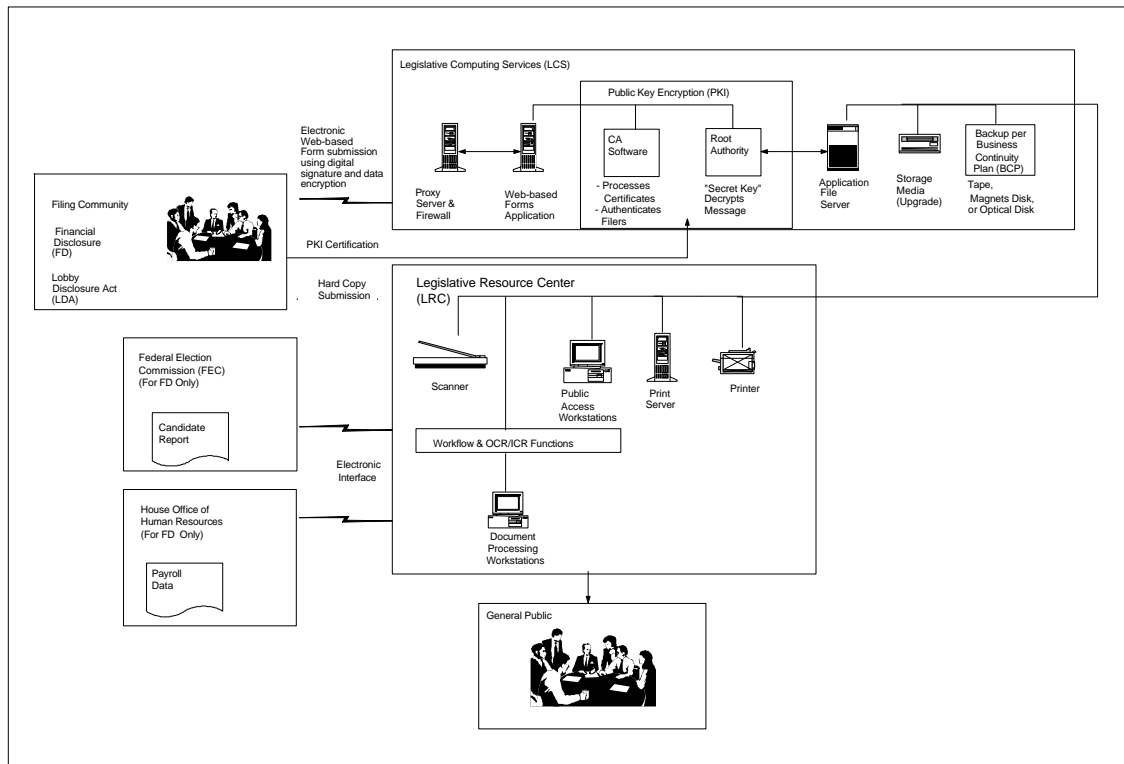


Figure 4.15: Alternative 4: Technology Overview

### Imaging/Workflow System Components

This alternative includes the technology components indicated in the previous alternative described in Section 3.1, Alternative 1: Imaging/Workflow System. Those technology components are summarized as the following:

- **Imaging/Workflow Application.** The imaging application is the engine that drives the scanning, indexing and report writing process. It executes the core functions of any document management system in an integrated manner. Most significant of the possible improvements to the core document imaging functionality is the workflow management and optical character features. Workflow functions manage a controlled flow of documents among administrators to ensure both accountability and quality assurance in the processing of information.
- **Storage Media and Backup.** Given the age and unreliable state of the existing WORM drive, upgrading to newer WORM technology implementing a digital-linear tape backup system should be considered, at a minimum.
- **Scanning and Printing Peripherals.** To plan for future processing loads, it may be necessary to upgrade the scanner and printing peripherals. The Clerk has made progress in this area by



procuring high speed Xerox Docutech printers capable of on-demand printing. This should reduce the Clerk's reliance on the GPO for specific publicly disseminated reports.

- **FEC and OHR Interfaces.** The automation of data that has been previously entered by hand is critical to improving data integrity and accuracy. Telecommunication links could be established with the FEC to allow for the timely upload of candidate data into the FD application. Although a high-speed telecommunication link is preferable, the alternative of loading the information via tape is a viable alternative. Automated interfaces could also be developed to accept payroll data from OHR for subsequent input into the FD application.

### **Electronic Filing Components**

This alternative includes the technology components indicated in the previous alternative described in Section 3.2, Alternative 2: Imaging/Workflow System with Electronic Filing and Basic Encryption. Those technology components are summarized as the following:

- **Web-based Forms Application.** A web-based forms application would be developed that would allow filers to dynamically fill out their FD and LDA forms.
- **Web Server Hardware/Software (SSL).** The web-based forms application detailed above would physically reside on a Internet web server within the confines of the LCS. This web server would have the capability to support encrypted connections initiated by the web clients (i.e., FD and LDA submission population) and through the use of a SSL connection.
- **Challenge/Response Mechanism.** Access to the FD and LDA web-based applications would be granted through a password and account ID mechanism. This challenge/response mechanism would authenticate users who choose to submit FD and LDA forms via the Internet using user IDs and passwords.
- **Proxy Server and Firewall.** A proxy server and firewall are required to protect the web server and web-based forms application from unauthorized uses by those wishing to infiltrate and disrupt the system.

### **Public Key Infrastructure Components**

If the Clerk develops and operates an in-house PKI, the PKI technology components described in Section 3.3, Alternative 3: Imaging/Workflow System with Electronic Filing and Outsourced PKI, would still be needed. Those technology components are summarized as the following:

- **Certificates.** This unique certificate, when provided with an electronic submission of the FD or LDA forms, would provide non-repudiation of identity of the filer.
- **Certificate Authority.** The primary function of the CA is to generate and manage the public key certificates that bind the user's identity with the user's public key. In order to perform this function, a CA must provide various services to the users of the certificates. Major services performed by a CA include certificate generation, authorization, and maintenance. CA products include GTE Cybertrust, Spyrus/Signet CA, Entrust WebCA, IBM Registry, and VeriSign On-Site.
- **Directory Servers.** The directory server is responsible for maintaining the actual certificates and user identification pairs for future authentication purposes.
- **Root Authority.** A Root Authority is the single point of trust at the top of a certification hierarchy of a PKI.

#### **4.3.4.3 High-Level Business Needs Evaluation**

This alternative was evaluated based on its ability to meet the high-level business needs as presented in Section 1.1.1 Needs Based Criteria. Figure 4.16: Alternative 4: Evaluation of High-Level Business Needs presents a summary of the evaluation of the high-level business needs.

Criteria	Criteria Rating	Comment
Input Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• <i>This alternative reduces the inefficiencies and errors associated with data input. Automated interfaces for files received from the FEC and the OHR would eliminate the need for manual keying of hard copy reports.</i></li> <li>• OCR/ICR functionality speeds the input of document index information.</li> </ul>
Processing Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Workflow functionality would improve quality assurance by providing the mechanism to administer controls associated with the FD and LDA processing cycle.</li> <li>• The core imaging system would incorporate logic to automate filer compliance.</li> </ul>
Output Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Standard report writing would be a component of the core imaging system.</li> <li>• The Xerox Docutech printer would be supported and allow for on-demand printing.</li> </ul>
Query Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Core system would include flexible, easy to use record query capabilities.</li> </ul>
Storage Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Image storage would be in a non-proprietary format.</li> </ul>
Technology Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• This alternative provides enhanced capabilities for electronic filing and signature verification. Implementation of PKI provides non-repudiation of electronic LDA and FD submissions. This functionality is not in the Imaging/Workflow System, with Electronic Filing and Basic Encryption alternative.</li> </ul>
Application Controls and Security Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• This alternative provides increased protection of data submitted electronically, along with non-repudiation assurances.</li> </ul>
Data Integrity Control Capabilities	<b>Fully</b>	<ul style="list-style-type: none"> <li>• Data integrity controls are improved through the use of workflow functionality and automated interfaces.</li> <li>• Field edits and error checking logic would be enhanced for all alternatives under consideration.</li> </ul>
<p>Key: <b>Partially</b>-Partially meets criteria    <b>Fully</b>-Fully meets criteria</p>		

*Figure 4.16: Alternative 4: Evaluation of High-Level Business Needs*

#### **4.3.4.4 Implementation Issues**

There are number of implementation issues that need to be considered when evaluating whether to implement an in-house PKI. The primary implementation issues are:

- **In-House PKI Implementation Issues.** The Clerk has the option of operating its own CA in-house or outsourcing some or most of the CA functions to a service provider, as described in the previous alternative. To operate the CA in-house, certificate management software is purchased from a vendor and used within the Clerk. The Clerk would operate the Registration Authority function, CA function, and all repository functions as well. A vendor could potentially provide training, installation and software support. Maintaining the PKI in-house would introduce many new areas of responsibility for the Clerk.
- **Clerk-Wide vs. House-Wide Implementation of PKI.** As described in the previous alternative, the Clerk should assess the investment costs associated with implementing a PKI infrastructure specific to the Clerk if House-wide



**Exhibit 5**  
**Cost-Benefit Analysis**



**Cost-Benefit Analysis**

**Table of Contents**

5.1. Methodology ..... 1

    5.1.1 System Alternative Cost Analysis ..... 1

        5.1.1.1 Development of Assumptions ..... 2

        5.1.1.2 Identification of Cost Factors..... 2

        5.1.1.3 Cost-Benefit Estimation of Alternatives ..... 3

    5.1.2 Cost Sensitivity Analysis..... 3

    5.1.3 Qualitative Analysis..... 4

5.2. System Alternative Cost Analysis..... 4

    5.2.1 Cost Analysis Summary ..... 5

    5.2.2 Existing System..... 7

        5.2.2.1 Non-Recurring Costs..... 8

        5.2.2.2 Recurring Costs..... 8

    5.2.3 Alternative 1: Imaging/Workflow System..... 11

        5.2.3.1 Non-Recurring Costs..... 11

        5.2.3.2 Recurring Costs..... 13

    5.2.4 Alternative 2: Imaging/Workflow System, with Electronic Filing and Basic Encryption ..... 15

        5.2.4.1 Non-Recurring Costs..... 16

        5.2.4.2 Recurring Costs..... 17

    5.2.5 Alternative 3: Imaging/Workflow, with Electronic Filing and an Outsourced PKI ..... 19

        5.2.5.1 Non-Recurring Costs..... 20

        5.2.5.2 Recurring Costs..... 21

    5.2.6 Alternative 4: Imaging/Workflow, with Electronic Filing and an In-house PKI..... 23

        5.2.6.1 Non-Recurring Costs..... 24

        5.2.6.2 Recurring Costs..... 25

5.3. Cost Sensitivity Analysis ..... 27

    5.3.1 Electronic Filing Efficiency Gains ..... 26

    5.3.2 Transition Cost Increases..... 28

5.4. Qualitative Analysis ..... 30





## **Cost-Benefit Analysis of Viable System Alternatives**

This exhibit presents the cost-benefit analysis for the four system alternatives that were identified as viable solutions for replacing the current Financial Disclosure (FD) and Lobby Disclosure Act (LDA) applications. This cost-benefit analysis includes a methodology section that identifies the resources used to collect information to identify cost factors, as well as the steps followed to analyze the costs and benefits of the viable system alternatives. The results presented include a cost comparison of the existing system and the four system alternatives. A cost sensitivity analysis and a qualitative analysis are also included.

### **5.1 Methodology**

The objective of the cost-benefit analysis was to analyze the viable system alternatives detailed in the Exhibit 4, *Feasibility Study* and to examine the costs and benefits for implementing each alternative. The cost-benefit analysis presents cost estimates for the existing system and the four viable system alternatives.

The cost-benefit analysis was based on a multi-step process that began with the development of assumptions and identification of cost factors, and resulted in a cost summary for the existing system and the four viable system alternatives. The multi-step process was composed of three steps listed below, followed by a description of each step:

- System Alternative Cost-Benefit Analysis.
- Cost Sensitivity Analysis.
- Qualitative Analysis.

#### **5.1.1 System Alternative Cost Analysis**

In Exhibit 4, *Feasibility Study*, information was presented on the viable system options for replacing the current FD and LDA system. For the cost-benefit analysis presented in this exhibit, estimated or preliminary cost data was collected and cost estimates were developed for inclusion in a cost model.

The cost model was used to analyze the costs of the existing system and the viable system alternatives. The cost data was collected from a variety of sources, including interviews with House personnel, software and hardware vendors, subject matter experts, and other legislative bodies. The cost analysis for the existing system and the four system alternatives comprised the following steps:

- Development of Assumptions.
- Identification of Cost Factors.

- Cost Comparison Analysis of Alternatives.

Each of the cost analysis steps is included below.

#### **5.1.1.1 Development of Assumptions**

The system alternatives cost analysis used the following general assumptions:

- **Salary and Fringe Benefits.** Actual salaries and an average fringe benefit rate of 29.55 percent for the personnel costs were used for salary and fringe benefit calculations for the existing system.<sup>21</sup> For personnel changes (additions or reductions), a salary of \$62,000 based on a Grade 10, Step 6 position as of January 1, 1998 was used.
- **Cost Factor Escalation.** Personnel costs (salary and fringe benefits) were escalated by 4 percent per year to represent cost-of-living increases.
- **Time Period of Analysis.** A five-year time period was used in this evaluation.<sup>22</sup>
- **Net Present Value and Discount Factor.** The net present value calculation was used to discount future costs using a discount rate of 7 percent.<sup>23</sup>

#### **5.1.1.2 Identification of Cost Factors**

The applicable cost factors listed below were identified by using the House's System Development Life Cycle (SDLC) procedures for performing a cost-benefit analysis and by using guidelines from the General Services Administration (GSA) Information Technology Planning and Investment Guide.

- **Non-recurring costs** are costs that occur in the first year of the analysis and are primarily costs for installation of software, software purchases and customization, hardware purchases, conversion/testing charges, training, and certificate management related charges. Non-recurring costs are assumed to be incurred during the first year of the analysis time period and are not discounted.

---

<sup>21</sup> The fringe benefit rate was obtained from OMB Circular A-76 for Executive Branch cost-benefit calculations.

<sup>22</sup> OMB Circular A-11 entitled *Preparation and Submission of Budget Estimates* and *The GSA Information Technology Planning and Investment Guide* prescribe a six-year planning horizon for IT investments. We reduced this time period to five years to be more conservative in our analysis with regard to the lifecycle of technology components.

<sup>23</sup> OMB Circular A-94 entitled *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs* indicates that a 7 percent discount factor should be used and that net present value is the standard criterion for deciding whether a Government program can be justified on economic principles.

- **Recurring costs** are costs that are incurred on an annual basis throughout the time period of the analysis, including the first year. The recurring costs include personnel salaries and fringe benefits, computer hardware (lease and maintenance), computer software (licenses and maintenance), and external vendor services. The recurring costs for each year are discounted using net present value.

#### **5.1.1.3 Cost-Benefit Estimation of Alternatives**

The cost estimates presented in this analysis are based on the following:

- **Vendor Quotes.** Vendors were contacted and the high-level requirements of the alternative systems were discussed to obtain software, hardware, and implementation costs. At least two vendor quotes were obtained for all estimates.
- **Independent Research Organizations.** Cost and product data from organizations such as Gartner Group, Faulkner, and Forrester were also collected.
- **Technology Specialists.** Specialists in imaging, electronic filing, and Public Key Infrastructure (PKI) technology were interviewed to develop and refine costs estimates for the alternatives.

The cost factors included in this evaluation represent the high-level “primary” costs to support the system alternatives. Cost factors not included in the evaluation include facilities and utility cost, personnel overhead, and supplies. The actual costs to implement the alternatives could vary significantly from these cost estimates during implementation due to the specific applications and requirements chosen by the Clerk. All cost estimates presented in this evaluation are rounded to the nearest thousand.

For this evaluation, benefits are defined as cost savings resulting from implementing the alternatives instead of continuing operation of the existing system. These benefits occur due to cost savings primarily from labor costs savings and reduced hardware and software maintenance costs. Benefits are included, where applicable, in the cost analysis of the alternatives and are represented as costs that are lower than the existing system.

#### **5.1.2 Cost Sensitivity Analysis**

The next step after performing the cost analysis was to perform a sensitivity analysis. This sensitivity analysis was performed to determine the impact of changes to the cost factors and assumptions used in this evaluation. The cost sensitivity analysis will provide management with additional information when analyzing the alternatives discussed in this evaluation.

### 5.1.3 Qualitative Analysis

A qualitative, or non-quantifiable, factor analysis was performed for each alternative. Qualitative factors were identified and assessed for each system alternative. The purpose of this analysis was to identify additional criteria factors to analyze the alternatives. The qualitative analysis methodology was composed of the following steps:

- **Identification of Qualitative Factors.** Six qualitative categories to assess the system alternatives were identified and defined: stakeholder needs and constraints, management control, security risk, commercial acceptance, Office of the Clerk (Clerk) organizational impact, and filing community impact. These categories represent qualitative, or non-quantifiable, attributes of the system alternatives.
- **Analysis of Qualitative Factors.** The six qualitative factors were analyzed for each alternative, and an assessment was developed that presented the issues associated with each factor.

## 5.2 System Alternative Cost Analysis

The system alternative cost analysis section presents the results of the cost analysis for the existing system and each system alternative. The cost analysis presentation is organized as follows:

- Cost Analysis Summary.
- Existing System.
- Imaging/Workflow System.
- Imaging/Workflow, with Electronic Filing and Basic Encryption.
- Imaging/Workflow, with Electronic Filing and an Outsourced<sup>24</sup> PKI.
- Imaging/Workflow, with Electronic Filing and an In-house PKI.

In each section, the non-recurring and recurring cost factors are discussed.

---

<sup>24</sup> For purposes of this study, outsourcing refers to administration of a system outside the confines of the Office of the Clerk. This could include outsourcing services provided by an external vendor or another House office (i.e., HIR).

### **5.2.1 Cost Analysis Summary**

Figure 5.1: Existing System and Alternative Costs Analysis on the following page presents a summary of the non-recurring and recurring cost estimates for the existing system and the four viable system alternatives. The figure presents five-year total cost estimates discounted using a present value calculation. This was done to provide an overall five-year lifecycle cost estimate of the existing system and each alternative.

As described in Exhibit 4, *Feasibility Study*, the alternatives build upon each other in terms of functionality and cost. For example, the estimated costs and functionality of the Imaging/Workflow alternative are included in all four alternatives. Additionally, the estimated costs and functionality for electronic filing in the Imaging/Workflow with Electronic Filing and Basic Encryption alternative are included in the remaining alternatives. The alternatives with PKI functionality differ only in terms of the estimated costs of outsourcing the PKI function versus maintaining the function in-house (by the Clerk).

Cost Factor	Existing System	Alternative 1	Alternative 2	Alternative 3	Alternative 4
		Imaging/Workflow System	Imaging/Workflow, w/Electronic Filing and Basic Encryption and PKI (Outsourced)	Imaging/Workflow, w/Electronic Filing, and PKI (Outsourced)	Imaging/Workflow, w/Electronic Filing, and PKI (In-house)
<b>1. Non-Recurring Costs</b>					
	\$0	\$20,000	\$20,000	\$28,000	\$32,000
Software	\$0	\$206,000	\$306,000	\$306,000	\$620,000
Hardware	\$0	\$77,000	\$95,000	\$107,000	\$107,000
Software	\$0	\$80,000	\$150,000	\$150,000	\$749,000
Training	\$0	\$5,000	\$11,000	\$14,000	\$41,000
CA Set-	\$0	\$0	\$0	\$120,000	\$0
<b>Total Non-Recurring Costs</b>	<b>\$0</b>	<b>\$388,000</b>	<b>\$582,000</b>	<b>\$725,000</b>	<b>\$1,549,000</b>
<b>2. Recurring Costs</b>					
<b>Personnel Salaries and Fringe Benefits</b>					
Legislative Resource Center (Forms	\$2,335,000	\$2,078,000	\$2,078,000	\$2,078,000	\$2,078,000
Legislative Computer Systems (Computer	\$126,000	\$483,000	\$839,000	\$839,000	\$1,195,000
House Information Resources (Mainframe	\$60,000	\$0	\$0	\$0	\$0
<b>Hardware (Lease and Maintenance)</b>					
Mainframe	\$126,000	\$0	\$0	\$0	\$0
OSAR Optical Disc Storage	\$134,000	\$0	\$0	\$0	\$0
Other Hardware	\$2,000	\$11,000	\$22,000	\$29,000	\$29,000
Scanner	\$107,000	\$0	\$0	\$0	\$0
New Scanner	\$0	\$23,000	\$23,000	\$23,000	\$23,000
New Optical Disc Storage	\$0	\$3,000	\$3,000	\$3,000	\$3,000
<b>Software (License and Maintenance)</b>					
Image System Software	\$7,000	\$0	\$0	\$0	\$0
RS-6000 Servers License/Operating	\$34,000	\$0	\$0	\$0	\$0
Other Software	\$47,000	\$26,000	\$69,000	\$69,000	\$69,000
PKI	\$0	\$0	\$0	\$0	\$890,000
New Imaging System	\$0	\$39,000	\$39,000	\$39,000	\$39,000
<b>External Vendor Services</b>					
PKI Vendor	\$0	\$0	\$0	\$305,000	\$0
<b>Total Recurring Costs</b>	<b>\$2,978,000</b>	<b>\$2,663,000</b>	<b>\$3,073,000</b>	<b>\$3,385,000</b>	<b>\$4,326,000</b>
<b>Total Estimated Costs</b>	<b>\$2,978,000</b>	<b>\$3,051,000</b>	<b>\$3,655,000</b>	<b>\$4,110,000</b>	<b>\$5,875,000</b>

Figure 5.1: Existing System<sup>25</sup> and Alternative Cost Analysis

The results of the cost analysis indicate that the estimated costs to implement each of the alternative systems are more expensive than the existing system over the five-year period. However, the alternatives do provide additional functionality over the existing system and better meet the evaluation criteria defined in this evaluation, as presented in Exhibit 4, *Feasibility Study*.

The total estimated costs for the **Imaging/Workflow System** are slightly higher than the existing system over the five-year period, primarily because of the non-recurring implementation costs.

<sup>25</sup> The total estimated costs for the existing system in this evaluation includes the costs associated with maintaining the FD and LDA applications as they are structured today. Because of the eventual migration off of the mainframe, HIR has investigated pursuing a solution that will serve during the interim between the time the applications are migrated off the mainframe and the time that the replacement solution for the FD and LDA applications are implemented. The potential interim solution involves porting the mainframe component of the FD and LDA application to a RS-6000 R/390 platform. The up-front costs (non-recurring) associated with this include approximately \$360,000 for hardware and software components. In addition, the potential recurring costs for the interim solution can be approximated as those attributed to the current mainframe component of the FD and LDA application (approximately \$126,000).

The recurring costs of the Imaging/Workflow System are less than the existing system recurring costs. For this alternative, we estimated that benefits would be achieved through lower recurring hardware and software maintenance costs.

The estimated costs for the **Imaging/Workflow System with Electronic Filing and Basic Encryption** are higher than the existing system, primarily because of the non-recurring implementation costs and the slightly higher recurring costs. For this alternative, it was estimated that benefits would be achieved through lower labor costs (in terms of salaries and fringe benefits) for forms processing. However, it was estimated that additional labor costs would be incurred for computer support due to the additional electronic filing functionality.

The estimated costs for both the **Imaging/Workflow System with Electronic Filing and an Outsourced PKI** and **Imaging/Workflow System with Electronic Filing and an In-House PKI** are significantly higher than the existing system. Both alternatives require significant non-recurring implementation costs and the recurring costs are higher than the existing system. The cost estimates for the In-House PKI alternative are significantly higher than the Outsourced PKI alternative due to the additional staff resources and software license and maintenance costs required.

The following discussion presents the cost analysis for the existing system and each of the four viable alternatives. The cost estimates presented are preliminary cost estimates and can be considered minimum costs that would be incurred in implementing the alternatives. Additionally, actual implementation of the alternatives may result in varied functionality and different technical components than those presented in this evaluation and would therefore differ in costs.

### **5.2.2 Existing System**

In the discussion below, the non-recurring and recurring cost estimates for this existing system are presented. Figure 5.2: Summary of Imaging/Workflow System Costs below summarizes the non-recurring and recurring cost estimates.



<b>Category</b>	<b>Estimated Costs</b>
Non-Recurring Costs	\$0
Recurring Costs	\$2,978,000
<b>Total Estimated Costs</b>	<b>\$2,978,000</b>

*Figure 5.2: Summary of Imaging/Workflow System Costs*

### **5.2.2.1 Non-Recurring Costs**

There are no non-recurring costs for the existing system. Costs associated with conversion/testing, software customization, hardware and software purchase, and training had been previously incurred when the existing system was originally developed. Thus, the non-recurring costs to develop the existing system are considered sunk costs and not included in the analysis of this existing system.

### **5.2.2.2 Recurring Costs**

Figure 5.3: Existing System - Recurring Cost Estimates on the following page presents the recurring cost estimates for the existing system. The recurring costs for the existing system were determined by reviewing current vendor invoices and by interviews with Legislative Resource Center (LRC) and Legislative Computer Systems (LCS) staff. The figure presents: the annual recurring cost estimates, and a five-year total of recurring costs discounted using the net present value calculation. These recurring costs are incurred on an annual basis throughout the five-year period of the analysis.

<b>Cost Factor</b>	<b>Annual Recurring Costs</b>	<b>5 Year Net Present Value Total</b>
<b>Personnel Salaries and Fringe Benefits</b>		
Legislative Resource Center (Forms Processing)	\$529,000	\$2,335,000
Legislative Computer Systems (Computer Support)	\$29,000	\$126,000
House Information Resources (Mainframe Support)	\$14,000	\$60,000
<b>Hardware (Lease and Maintenance)</b>		
Mainframe Costs	\$30,000	\$126,000
OSAR Optical Disc Storage Maintenance	\$32,000	\$134,000
Other Hardware Maintenance	\$1,000	\$2,000
Scanner License/Maintenance	\$25,000	\$107,000
New Scanner License/Maintenance	\$0	\$0
New Optical Disc Storage Maintenance	\$0	\$0
<b>Software (License and Maintenance)</b>		
Image System Software License/Maintenance	\$2,000	\$7,000
RS-6000 Servers License/Operating System	\$8,000	\$34,000
Other Software License/Maintenance	\$11,000	\$47,000
PKI Annual License/Maintenance	\$0	\$0
New Imaging System Maintenance	\$0	\$0
<b>External Vendor Services</b>		
PKI Vendor Hosting	\$0	\$0
<b>Total Recurring Costs</b>	<b>\$681,000</b>	<b>\$2,978,000</b>

*Figure 5.3: Existing System - Recurring Cost Estimates*

### **Personnel Salaries and Fringe Benefits**

The recurring personnel salaries and fringe benefits for the existing system include the staff to support the current FD and LDA applications. Personnel from the LRC, LCS, and House Information Resources (HIR) currently support the existing system. Listed below is a description of the staff resources dedicated to supporting the FD and LDA applications from the associated House office.

- **Legislative Resource Center** staff dedicated to processing the FD and LDA submissions include seven full-time staff and approximately 50 percent of the efforts of another four full-time staff.

- **Legislative Computer Systems** staff dedicated to maintaining the computer systems associated with the FD and LDA applications include 40 percent of the efforts of one full-time staff member.
- **House Information Resources** staff dedicated to maintaining the mainframe component of the FD and LDA system includes approximately 20 percent of the efforts of one full-time staff member.

#### **Hardware (Lease and Maintenance)**

The recurring hardware lease and maintenance costs for the existing system include the costs associated with operating the mainframe system, maintaining the OSAR optical disc storage system, and licensing and maintaining two scanners used for forms processing. The specific cost factors for the existing system and the four alternatives include:

- **Mainframe Costs** includes the lease and maintenance costs associated with the mainframe hardware.
- **OSAR Optical Disk Storage Maintenance** includes the maintenance costs for the optical disk storage system.
- **Other Hardware Maintenance** includes any other related peripheral hardware.
- **Scanner License and Maintenance** includes the license and maintenance fees associated with the current scanners.
- **New Scanner License and Maintenance** includes the license and maintenance costs for the new scanners, where pertinent.
- **New Optical Disk Storage Maintenance** includes the license and maintenance costs for the new optical storage system, where pertinent.

#### **Software (License and Maintenance)**

The recurring software license and maintenance costs for the existing system include the costs associated with the current image system software and RS-6000 license and maintenance fees. This cost category also includes maintenance and license fees for other software associated with the existing system (i.e., database management software and printer servers). The specific cost factors for the existing system and the four alternatives include:

- **Image System Software License and Maintenance** includes the license and maintenance costs associated with the current imaging system.

- **RS-6000 Server License and Operating System** includes the license and maintenance fees associated with the current RS-6000 servers and operating system.
- **Other Software License and Maintenance** includes the license and maintenance fees for other system software components.
- **PKI Annual License and Maintenance** includes the annual license and maintenance fees associated with a PKI. The existing system does not include these functions.
- **New Imaging System Maintenance** includes the maintenance fees associated with the new imaging system software.

### External Vendor Services

External vendor services are not used in the existing system.<sup>26</sup>

### 5.2.3 Alternative 1: Imaging/Workflow System

In the discussion below, the non-recurring and recurring cost estimates for this alternative are presented. Figure 5.4: Summary of Imaging/Workflow Costs below summarizes the non-recurring and recurring cost estimates.

<b>Category</b>	<b>Estimated Costs</b>
Non-Recurring Costs	\$388,000
Recurring Costs	\$2,663,000
<b>Total Estimated Costs</b>	<b>\$3,051,000</b>

*Figure 5.4: Summary of Imaging/Workflow System Costs*

#### 5.2.3.1 Non-Recurring Costs

Figure 5.5: Imaging/Workflow System - Non-Recurring Cost Estimates below presents the non-recurring cost estimates for the Imaging/Workflow System alternative. The figure presents cost estimates that would be incurred to support a new imaging/workflow system for the FD and LDA applications. These non-recurring costs are incurred during the first year of the alternative. Each of the cost factors is discussed below.

---

<sup>26</sup> For the purposes of this study, the External Vendor Services costs category only includes costs associated with PKI Vendor Hosting.

<b>Cost Factor</b>	<b>Estimated Costs</b>
Conversion/Testing	\$20,000
Software Integration/Customization	\$206,000
Hardware Purchase	\$77,000
Software Purchase	\$80,000
Training	\$5,000
CA Set-Up/Initialization	\$0
<b>Total</b>	<b>\$388,000</b>

*Figure 5.5: Imaging/Workflow System - Non-Recurring Cost Estimates*

### **Conversion/Testing**

This cost category includes the estimated costs to convert the approximately 157 gigabytes of image data stored on 12'' Write-One-Read-Many (WORM) optical storage platters to the 5.2GB WORM optical storage disks. This cost factor was estimated based on a vendor quote for data conversion services.

### **Software Integration/Customization**

This cost category includes the estimated costs to customize the workflow scripts and document capture processes associated with the application workflow module, to develop programs for supporting the OCR/ICR processing module, and also to develop the automated interfaces with the Federal Election Commission (FEC) and the Office of Human Resources (OHR). Costs for software integration/customization for this alternative was based on estimates derived from knowledge obtained from similarly scoped projects.<sup>27</sup>

### **Hardware Purchase**

This cost category includes the estimated costs associated with purchasing the magneto-optical disc storage unit and one additional external magneto-optical disk drive. Also included are 5.2GB optical storage disks, two peripheral scanners and two workstations for the imaging system. This cost category also includes the estimated costs for the purchase of a digital-linear tape backup system. The estimated costs for the hardware components for this alternative were obtained from vendor quotes.

### **Software Purchases**

This cost category includes the estimated cost to purchase the software utilities required for the imaging/workflow system. This includes software used for the optical disk storage unit, the

---

<sup>27</sup> A total of 2,000 hours was estimated for completing the software integration/customization for this alternative.

imaging system, the scanners, and the OCR/ICR processing engine. The cost estimates were based on vendor quotes.

### **Training**

This cost category includes the estimated cost for a vendor administered imaging system and OCR/ICR forms processing training course for two staff members. The estimated costs for the hardware components for this alternative were obtained from vendor quotes.

### **Certificate Authority (CA) Set-Up/Initialization**

This cost category refers to establishing an external certificate authority and is applicable only in Alternative 3.

### **5.2.3.2 Recurring Costs**

Figure 5.6: Imaging/Workflow System - Recurring Cost Estimates below presents the recurring cost estimates for this alternative. The figure presents the annual recurring cost estimates, and a five-year total of recurring costs discounted using the net present value calculation. These recurring costs are incurred on an annual basis throughout the five-year period of the analysis.

<b>Cost Factor</b>	<b>Annual Recurring Costs</b>	<b>5 Year Net Present Value Total</b>
<b>Personnel Salaries and Fringe Benefits</b>		
Legislative Resource Center (Forms Processing)	\$470,000	\$2,078,000
Legislative Computer Systems (Computer Support)	\$109,000	\$483,000
House Information Resources (Mainframe Support)	\$0	\$0
<b>Hardware (Lease and Maintenance)</b>		
Mainframe Costs	\$0	\$0
OSAR Optical Disc Storage Maintenance	\$0	\$0
Other Hardware Maintenance	\$3,000	\$11,000
Scanner License/Maintenance	\$0	\$0
New Scanner License/Maintenance	\$6,000	\$23,000
New Optical Disc Storage Maintenance	\$1,000	\$3,000
<b>Software (License and Maintenance)</b>		
Image System Software License/Maintenance	\$0	\$0
RS-6000 Servers License/Operating System	\$0	\$0
Other Software License/Maintenance	\$6,000	\$26,000
PKI Annual License/Maintenance	\$0	\$0
New Imaging System Maintenance	\$10,000	\$39,000
<b>External Vendor Services</b>		
PKI Vendor Hosting	\$0	\$0
<b>Total Recurring Costs</b>	<b>\$605,000</b>	<b>\$2,663,000</b>

*Figure 5.6: Imaging/Workflow System - Recurring Cost Estimates*

### **Personnel Salaries and Fringe**

The recurring personnel salaries and fringe benefits for this alternative include the staff to support the new FD and LDA applications from the LRC and LCS. Listed below is a description of the staff resources dedicated to supporting this alternative.

- **Legislative Resource Center** staff dedicated to processing the FD and LDA submissions for this alternative include a reduction of 20 percent in forms processing labor resources from the existing system due to the estimated efficiencies gained by this technology.<sup>28</sup>

<sup>28</sup> The efficiencies associated with the new imaging system have been estimated to provide a reduction in staff resources by approximately 20 percent. Processing staff were reduced from seven to six to reflect this 20 percent increase in efficiency.

- **Legislative Computer Systems** staff dedicated to maintaining the computer systems associated with the FD and LDA applications include the addition of one full-time System Administrator position to the LCS staff. The additional System Administration position is being created to assist with maintaining the additional system complexities associated with this alternative.
- **House Information Resources** staff resources are eliminated because the mainframe component of the existing system is no longer necessary.

### **Hardware (Lease and Maintenance)**

The primary difference in the recurring hardware costs from the existing system is the elimination of the lease and maintenance costs for the current FileNet optical storage system and the costs associated with the Bell & Howell and the Kodak scanners<sup>29</sup> currently used in the LRC. These three components would be replaced with a new optical storage system and two new scanners that have less recurring costs for license and maintenance. Lease and maintenance costs for other hardware components, such as servers and a tape backup system, are also included in this cost category.

### **Software (License and Maintenance)**

The recurring software costs for this alternative would include the elimination of the costs associated with the FileNet imaging system and the RS-6000 server and operating system license/maintenance. Software lease and maintenance fees for a new imaging system and for other related software programs are included in this cost category.

### **External Vendor Services**

External vendor services are not pertinent since the use of external vendors is not part of this alternative.

## **5.2.4 Alternative 2: Imaging/Workflow System, with Electronic Filing and Basic Encryption**

In the discussion below, non-recurring and recurring cost estimates for this alternative are presented. These estimates include both the cost and functionality as described in Section E.2.3, Imaging/Workflow System of this evaluation. Figure 5.7: Summary of Imaging/Workflow System, with Electronic Filing and Basic Encryption Costs below summarizes these estimated costs.

---

<sup>29</sup> It is assumed for the evaluation that all new hardware components would be purchased to replace existing components. After a more detailed requirements analysis, the extent to which components can be re-used would be determined.



Category	Estimated Costs
Non-Recurring Costs	\$582,000
Recurring Costs	\$3,073,000
<b>Total Estimated Costs</b>	<b>\$3,655,000</b>

*Figure 5.7: Summary of Imaging/Workflow System, with Electronic Filing and Basic Encryption Costs*

#### 5.2.4.1 Non-Recurring Costs

Figure 5.8: Imaging/Workflow System, with Electronic Filing and Basic Encryption– Non-Recurring Costs Estimates below presents the non-recurring cost estimates for this alternative. The figure presents cost estimates that would be incurred to support a new imaging/workflow system and electronic filing with basic encryption for the FD and LDA applications. These non-recurring costs are incurred during the first year of the alternative.

Cost Factor	Estimated Costs
Conversion/Testing	\$20,000
Software Integration/Customization	\$306,000
Hardware Purchase	\$95,000
Software Purchase	\$150,000
Training	\$11,000
CA Set-Up/Initialization	\$0
<b>Total</b>	<b>\$582,000</b>

*Figure 5.8: Imaging/Workflow System, with Electronic Filing and Basic Encryption–*

#### Non-Recurring Cost Estimates

##### Conversion/Testing

This cost category does not introduce any new conversion/testing costs, but does include those noted in the previous alternative: conversion of image data from optical storage platters to optical storage disks.

##### Software Integration/Customization

This cost category includes the estimated costs to customize the web-based forms application used for electronic submission of FD and LDA forms. The customization costs were determined by a vendor estimate based on projects of similar scope. The software integration/customization cost category also contains the following costs as noted in the previous alternative: customization of the workflow scripts and document capture processes associated with the workflow

application, programs for OCR/ICR processing, and the development of an automated interface with FEC and OHR.

### **Hardware Purchase**

This cost category includes the estimated costs associated with the purchase of a web and firewall server, and an index database management server. The estimated costs for the hardware components for this alternative were obtained from vendor quotes. The hardware purchase category for this alternative also contains the following costs as noted in the previous alternative: magneto-optical disc storage unit, one additional external magneto-optical disk drive, optical storage disks, two peripheral scanners and two workstations for the imaging system, and a digital-linear tape backup system.

### **Software Purchases**

This cost category includes the estimated costs for the index database management system, the Internet firewall, and the web-based forms authoring software. The estimated costs for the software components for this alternative were obtained from vendor quotes. The software purchase category for this alternative also contains the following costs as noted in the previous alternative: software utilities for the imaging/workflow, the optical disk storage unit, the scanners, and the OCR/ICR processing engine.

### **Training**

This cost category includes the estimated cost for three staff members to attend a vendor-administered course for web-based forms authoring. The estimated costs for the training associated with this alternative were obtained from vendor quotes. This cost category also contains the cost for an OCR/ICR forms processing training course for two staff members as noted in the previous alternative.

### **CA Set-Up/Initialization**

This cost category refers to establishing an external certificate authority and is applicable only in Alternative 3.

#### **5.2.4.2 Recurring Costs**

Figure 5.9: Imaging/Workflow System, with Electronic Filing and Basic Encryption - Recurring Costs Estimates below presents the recurring cost estimates for this alternative. The figure presents the annual recurring cost estimates, and a five-year total of recurring costs discounted using the net present value calculation. These recurring costs are incurred on an annual basis throughout the five-year period of the analysis. Discussion of the recurring cost components associated with this alternative is included on the following page.

<b>Cost Factor</b>	<b>Annual Recurring Costs</b>	<b>5 Year Net Present Value Total</b>
<b>Personnel Salaries and Fringe Benefits</b>		
Legislative Resource Center (Forms Processing)	\$470,000	\$2,078,000
Legislative Computer Systems (Computer Support)	\$190,000	\$839,000
House Information Resources (Mainframe Support)	\$0	\$0
<b>Hardware (Lease and Maintenance)</b>		
Mainframe Costs	\$0	\$0
OSAR Optical Disc Storage Maintenance	\$0	\$0
Other Hardware Maintenance	\$6,000	\$22,000
Scanner License/Maintenance	\$0	\$0
New Scanner License/Maintenance	\$6,000	\$23,000
New Optical Disc Storage Maintenance	\$1,000	\$3,000
<b>Software (License and Maintenance)</b>		
Image System Software License/Maintenance	\$0	\$0
RS-6000 Servers License/Operating System	\$0	\$0
Other Software License/Maintenance	\$16,000	\$69,000
PKI Annual License/Maintenance	\$0	\$0
New Imaging System Maintenance	\$10,000	\$39,000
<b>External Vendor Services</b>		
PKI Vendor Hosting	\$0	\$0
<b>Total Recurring Costs</b>	<b>\$699,000</b>	<b>\$3,073,000</b>

*Figure 5.9: Imaging/Workflow System, with Electronic Filing and Basic Encryption-  
Recurring Cost Estimates*

### **Personnel Salaries and Fringe Benefits**

The recurring personnel salaries and fringe benefits for this alternative include the staff to support the current FD and LDA applications from the LRC and LCS. Listed below is a description of the staff resources dedicated to supporting this alternative.

- **Legislative Resource Center** staff dedicated to processing the FD and LDA submissions for this alternative include a reduction of 20 percent in forms processing labor resources from the existing system due to the estimated efficiencies gained by the imaging/workflow technology. The electronic filing functionality introduced by this alternative may also present efficiencies.<sup>30</sup>

<sup>30</sup> Although the implementation of electronic filing technology would be expected to generate efficiencies from

- **Legislative Computer Systems** staff dedicated to maintaining the computer systems associated with the FD and LDA applications include 40 percent of the efforts of one full-time staff member and the addition of two System Administrator positions to the LCS staff. The additional System Administration positions are being created to assist with maintaining the additional system complexities associated with this alternative.
- **House Information Resources** staff resources are eliminated because the mainframe component of the existing system is no longer necessary.

**Hardware (Lease and Maintenance)**

Estimated lease and maintenance costs for other hardware components, such as servers, are included in this cost category. Also included in this cost category are costs noted in the previous alternative for the following: hardware license/maintenance costs for the new optical storage system, two new scanners, and a tape backup system.

**Software (License and Maintenance)**

Estimated license and maintenance costs for the software components associated with the web-based forms application are included in this cost category. Also included in this category are costs noted in the previous alternative for the following: software maintenance fees for a new imaging system and other related software.

**External Vendor Services**

External vendor services are not pertinent since the use of external vendors is not part of this alternative.

**5.2.5 Alternative 3: Imaging/Workflow, with Electronic Filing and an Outsourced PKI**

The non-recurring and recurring cost estimates for this alternative are presented in the discussion below. Figure 5.10: Summary of Imaging/Workflow with Electronic Filing and an Outsourced PKI Costs below summarizes these estimated costs for this alternative. These estimated costs also include both the cost and functionality as described in Section 5.2.4, Imaging/Workflow System, with Electronic Filing and Basic Encryption, of this evaluation.

<b>Category</b>	<b>Estimated Costs</b>
Non-Recurring Costs	\$725,000
Recurring Costs	\$3,385,000

---

reduced data entry of hard copy forms, the specific amount of labor cost savings is unclear. Therefore, we have not made any assumptions with regard to labor cost efficiencies from electronic filing. However, we do provide an analysis on potential efficiencies in Section 5.3, Cost Sensitivity Analysis.

<b>Total Estimated Costs</b>	<b>\$4,110,000</b>
------------------------------	--------------------

*Figure 5.10: Summary of Imaging/Workflow with Electronic Filing and an Outsourced PKI Costs*

### 5.2.5.1 Non-Recurring Costs

Figure 5.11: Imaging/Workflow System with Electronic Filing and an Outsourced PKI – Non-Recurring Cost Estimates below presents the non-recurring cost estimates for this alternative. The figure below presents cost estimates that would be incurred to support a new imaging/workflow with electronic filing and an outsourced PKI for the LDA and FD applications. These non-recurring costs are incurred during the first year of the alternative.

<b>Cost Factor</b>	<b>Estimated Costs</b>
Conversion/Testing	\$28,000
Software Integration/Customization	\$306,000
Hardware Purchase	\$107,000
Software Purchase	\$150,000
Training	\$14,000
CA Set-Up/Initialization	\$120,000
<b>Total</b>	<b>\$725,000</b>

*Figure 5.11: Imaging/Workflow System with Electronic Filing and an Outsourced PKI – Non-Recurring Cost Estimates*

#### **Conversion/Testing**

This cost category includes the estimated costs associated with systems testing.<sup>31</sup> The conversion/testing costs factor for this alternative also contains the following cost as noted in the previous alternative: the conversion of image data from optical storage platters to optical storage disks.

#### **Software Integration/Customization**

This cost category does not introduce any new software/customization costs, but does include costs that were presented in the previous alternative for the following: customization of the workflow scripts, integration of the document capture processes associated with the workflow application, and customization of web-based forms application.

#### **Hardware Purchase**

---

<sup>31</sup> When determining the conversion/testing costs for the outsourced PKI, it was assumed that some system functions would remain with the Clerk. Thus, system testing would need to be performed.

This cost category includes costs for the purchase of two servers to house the PKI related certificate management and directory functions. The hardware purchase costs category factor for this alternative also contains the following costs as noted in the previous alternative: a magneto-optical disc storage unit, one additional external magneto-optical disk drive, optical storage disks, two peripheral scanners, two workstations for the imaging system, a digital-linear tape backup system, web and firewall servers, and an index database management server.

### **Software Purchase**

There are no new software purchase costs associated with an outsourced PKI. The software purchase cost category for this alternative contains the following costs as noted in the previous alternative: software utilities for the imaging/workflow, the optical disk storage unit, the scanners, OCR/ICR processing engine, an index database management system, the Internet firewall, and the web-based forms authoring software.

### **Training**

This cost category includes the estimated costs for a two-day PKI orientation class for two staff members. The estimated training costs for this alternative were obtained from vendor quotes. This cost category for this alternative also contains the following costs as noted in the previous alternative: OCR/ICR forms processing training course for two staff members, and web-based forms authoring training course for three staff members.

### **CA Set-Up/Initialization**

This costs category includes the estimated costs associated with establishing the PKI service with an outsourcing vendor.

#### **5.2.5.2 Recurring Costs**

Figure 5.12: Imaging/Workflow System with Electronic Filing and an Outsourced PKI - Recurring Cost Estimates below presents the recurring cost estimates for this alternative. The figure presents the annual recurring cost estimates, and a five-year total of recurring costs discounted using the net present value calculation. These recurring costs are incurred on an annual basis throughout the five-year period of the analysis.

<b>Cost Factor</b>	<b>Annual Recurring Costs</b>	<b>5 year Net Present Value Total</b>
<b>Personnel Salaries and Fringe Benefits</b>		
Legislative Resource Center (Forms Processing)	\$470,000	\$2,078,000
Legislative Computer Systems (Computer Support)	\$190,000	\$839,000
House Information Resources (Mainframe Support)	\$0	\$0
<b>Hardware (Lease and Maintenance)</b>		
Mainframe Costs	\$0	\$0
OSAR Optical Disc Storage Maintenance	\$0	\$0
Other Hardware Maintenance	\$8,000	\$29,000
Scanner License/Maintenance	\$0	\$0
New Scanner License/Maintenance	\$6,000	\$23,000
New Optical Disc Storage Maintenance	\$1,000	\$3,000
<b>Software (License and Maintenance)</b>		
Image System Software License/Maintenance	\$0	\$0
RS-6000 Servers License/Operating System	\$0	\$0
Other Software License/Maintenance	\$16,000	\$69,000
PKI Annual License/Maintenance	\$0	\$0
New Imaging System Maintenance	\$10,000	\$39,000
<b>External Vendor Services</b>		
PKI Vendor Hosting	\$74,000	\$305,000
<b>Total Recurring Costs</b>	<b>\$775,000</b>	<b>\$3,385,000</b>

*Figure 5.12: Imaging/Workflow System with Electronic Filing and an Outsourced PKI - Recurring Cost Estimates*

### **Personnel Salaries and Fringe Benefits**

The recurring personnel salaries and fringe benefits for this alternative include the staff to support the current FD and LDA applications from the LRC and LCS. Listed below is a description of the staff resources dedicated to supporting this alternative.

- **Legislative Resource Center** staff dedicated to processing the FD and LDA submissions for this alternative include a reduction of resources by 20 percent due to the efficiencies gained by the imaging technology. The functionality introduced by this alternative may also present other efficiencies associated with electronic filing.

- **Legislative Computer Systems** staff dedicated to maintaining the FD and LDA computer systems includes 40 percent of the efforts of one full-time staff member, and the addition of one System Administrator position and one staff member dedicated to certificate management functions. The additional positions for this alternative are being created to assist with maintaining the additional system complexities associated with this alternative.
- **House Information Resources** staff resources are eliminated because the mainframe component of the existing system is no longer necessary.

**Hardware (Lease and Maintenance)**

Estimated lease and maintenance costs for other hardware components, such as servers, are included in this cost category. Also included in this cost category are costs noted in the previous alternative for the following: the hardware license/maintenance costs for the new optical storage system and the two new scanners.

**Software (License and Maintenance)**

This cost category does not introduce any new costs, but does include the software maintenance fees for a new imaging system cost as noted in the previous alternative.

**External Vendor Services**

Estimated costs for PKI vendor hosting services under this alternative is included in this cost category.

**5.2.6 Alternative 4: Imaging/Workflow, with Electronic Filing and an In-house PKI**

In the discussion below, the non-recurring and recurring cost estimates for this alternative are presented. Figure 5.13: Summary of the Imaging/Workflow with Electronic Filing and an In-house PKI Costs below summarizes these estimated costs for this alternative. These estimated costs also include both the cost and functionality as described in Section 5.2.4, Imaging/Workflow System, with Electronic Filing and Basic Encryption, of this evaluation.

<b>Category</b>	<b>Estimated Costs</b>
Non-Recurring Costs	\$1,549,000
Recurring Costs	\$4,326,000
<b>Total Estimated Costs</b>	<b>\$5,875,000</b>

*Figure 5.13: Summary of the Imaging/Workflow with Electronic Filing and an In-house PKI Costs*



### 5.2.6.1 Non-Recurring Costs

Figure 5.14: Imaging/Workflow System with Electronic Filing and an In-house PKI – Non-Recurring Cost Estimates below presents the non-recurring cost estimates for this alternative. The figure below presents cost estimates that would be incurred to support a new imaging/workflow with electronic filing and an in-house PKI environment for the LDA and FD applications. These non-recurring costs are incurred during the first year of the alternative.

<b>Cost Factor</b>	<b>Estimated Costs</b>
Conversion/Testing	\$32,000
Software Integration/Customization	\$620,000
Hardware Purchase	\$107,000
Software Purchase	\$749,000
Training	\$41,000
CA Set-Up/Initialization	\$0
<b>Total</b>	<b>\$1,549,000</b>

*Figure 5.14: Imaging/Workflow System with Electronic Filing and an In-house PKI – Non-Recurring Cost Estimates*

#### **Conversion/Testing**

This cost category includes the estimated costs for systems testing for the PKI environment. These estimated costs for conversion/testing were obtained from vendor quotes. The conversion/testing cost category also includes the following costs as presented in the previous alternative: conversion of image data from optical storage platters to optical storage disks.

#### **Software Integration/Customization**

This cost category includes the estimated costs to install and integrate the software modules for the PKI environment.<sup>32</sup> The software integration/customization cost category also includes the following costs as presented in the previous alternative: customization of the workflow scripts, integration of the document capture processes associated with the workflow application, and customization of web-based forms application.

#### **Hardware Purchase**

This cost category includes the estimated costs to purchase two servers dedicated to the in-house PKI environment. The estimated costs for the hardware purchase for this alternative was

---

<sup>32</sup> “Pricing Public Key Infrastructure”, September 8, 1998, Gartner Group, provides recommendations for integration costs for PKI projects ranging from 20 to 50 percent of project costs. For the purposes of this evaluation, 50 percent was used.

obtained from vendor quotes. The hardware purchase cost category also includes the following costs as presented in the previous alternative: a magneto-optical disc storage unit, one additional external magneto-optical disk drive, optical storage disks, two peripheral scanners, two workstations for the imaging system, a digital-linear tape backup system, web and firewall servers, and an index database management server.

### **Software Purchase**

This cost category includes the estimated costs to purchase the software components to perform the PKI certificate management and directory functions. The estimated costs for the software purchase for this alternative were obtained from vendor quotes. The software purchase costs category also includes the following costs as presented in the previous alternative: purchase of software utilities for the imaging/workflow, the optical disk storage unit, the scanners, and the OCR/ICR processing engine, an index database management system, the Internet firewall, and the web-based forms authoring software.

### **Training**

This cost category includes the estimated costs for a five-day PKI orientation course for six staff members. The estimated training costs for this alternative were obtained from vendor quotes. This cost category also includes the following costs as presented in the previous alternative: OCR/ICR forms processing training course for two staff members, and web-based forms authoring training course for three staff members.

### **CA Set-Up/Initialization**

This cost category refers to establishing an external certificate authority and is applicable only in Alternative 3.

#### **5.2.6.2 Recurring Costs**

Figure 5.15: Imaging/Workflow System with Electronic Filing and an In-house PKI –Recurring Cost Estimates on the following page presents the recurring cost estimates for this alternative. The figure presents the annual recurring cost estimates, and a five-year total of recurring costs discounted using the net present value calculation. These recurring costs are incurred on an annual basis throughout the five-year period of the analysis.

<b>Cost Factor</b>	<b>Annual Recurring Costs</b>	<b>5 Year Net Present Value Total</b>
<b>Personnel Salaries and Fringe Benefits</b>		
Legislative Resource Center (Forms Processing)	\$470,000	\$2,078,000
Legislative Computer Systems (Computer Support)	\$313,000	\$1,195,000
House Information Resources (Mainframe Support)	\$0	\$0
<b>Hardware (Lease and Maintenance)</b>		
Mainframe Costs	\$0	\$0
OSAR Optical Disc Storage Maintenance	\$0	\$0
Other Hardware Maintenance	\$8,000	\$29,000
Scanner License/Maintenance	\$0	\$0
New Scanner License/Maintenance	\$6,000	\$23,000
New Optical Disc Storage Maintenance	\$1,000	\$3,000
<b>Software (License and Maintenance)</b>		
Image System Software License/Maintenance	\$0	\$0
RS-6000 Servers License/Operating System	\$0	\$0
Other Software License/Maintenance	\$16,000	\$69,000
PKI Annual Maintenance/License	\$217,000	\$890,000
New Imaging System Maintenance	\$10,000	\$39,000
<b>External Vendor Services</b>		
PKI Vendor Hosting	\$0	\$0
<b>Total Recurring Costs</b>	<b>\$1,041,000</b>	<b>\$4,326,000</b>

*Figure 5.15: Imaging/Workflow System with Electronic Filing and an In-house PKI –  
Recurring Cost Estimates*

### **Personnel Salaries and Fringe Benefits**

The recurring personnel salaries and fringe benefits for this alternative include the staff to support the current FD and LDA applications from the LRC and LCS. Listed below is a description of the staff resources dedicated to supporting this alternative.

- **Legislative Resource Center** staff dedicated to processing the FD and LDA submissions for this alternative include a reduction of resources by 20 percent due to the efficiencies gained by the imaging/workflow technology. The functionality introduced by this alternative may also present other efficiencies associated with electronic filing.

- **Legislative Computer Systems** staff dedicated to maintaining the FD and LDA computer system includes 40 percent of the efforts of one full-time staff member, and the addition of two System Administrator positions and one staff member dedicated to certificate management functions for the in-house PKI scenario.
- **House Information Resources** staff resources are eliminated because the mainframe component of the existing system is no longer necessary.

### **Hardware (Lease and Maintenance)**

This cost category includes estimated costs associated with hardware lease and maintenance costs for the servers associated with this alternative. The hardware lease and maintenance costs category also includes costs noted in the previous alternative for the following: the hardware license/maintenance costs for the new optical storage system, and the two new scanners.

### **Software (License and Maintenance)**

The software license and maintenance costs for this alternative includes estimated annual charges for the in-house PKI related software. This estimated cost includes charges for the certificate management software and digital certificate license fees. This alternative also includes the software lease and maintenance costs noted in the previous alternative for the software maintenance fees for a new imaging system.

### **External Vendor Services**

External vendor services are not pertinent since the use of external vendors is not part of this alternative.

## **5.3 Cost Sensitivity Analysis**

A sensitivity analysis was conducted on the estimated costs (non-recurring and recurring) for the four viable alternatives analyzed in this exhibit. The objective of the sensitivity analysis was to analyze changes to assumptions to determine the impact on the overall cost of the alternatives. Two scenarios for the sensitivity analysis were developed: Electronic Filing Efficiency Gains, and Increased Transition Costs which are presented below.

### **5.3.1 Electronic Filing Efficiency Gains**

With the introduction of electronic filing capabilities, efficiencies may be realized with regards to the processing of the FD and LDA submissions. These efficiencies would occur primarily because of a reduction in hard copy form submissions. Areas where the greatest efficiencies could occur include the elimination of the scan and index functions associated with the current

forms processing. However, the exact extent of the efficiencies would depend on the number of filers that choose to file electronically.

In order to analyze the potential impact of efficiencies from electronic filing on the cost of the alternatives, the personnel salaries and fringe benefits cost factor associated with forms processing (LRC) for the three electronic filing alternatives were decreased by 25 percent.<sup>33</sup>

Figure 5.16: Sensitivity Analysis - Electronic vs. Hardcopy Submission Efficiency Gains on the following page presents the results of the sensitivity analysis for this scenario. The results indicate that the total estimated costs for two alternatives — Imaging/Workflow with Electronic Filing and Basic Encryption and Imaging/Workflow with Electronic Filing and an Outsourced PKI — are now only slightly higher than the existing system and the Image/Workflow System.

Cost Factor	Existing System	Alternative 1	Alternative 2	Alternative 3	Alternative 4
		Imaging/Workflow System	Imaging/Workflow, w/Electronic Filing and Basic Encryption	Imaging/Workflow, w/Electronic Filing, and PKI (Outsourced)	Imaging/Workflow, w/Electronic Filing, and PKI (In-house)
<b>1. Non-Recurring Costs</b>					
Conversion/Testing	\$0	\$20,000	\$20,000	\$28,000	\$32,000
Software Integration/Customization	\$0	\$206,000	\$306,000	\$306,000	\$620,000
Hardware Purchase	\$0	\$77,000	\$95,000	\$107,000	\$107,000
Software Purchase	\$0	\$80,000	\$150,000	\$150,000	\$749,000
Training	\$0	\$5,000	\$11,000	\$14,000	\$41,000
CA Set-Up/Initialization	\$0	\$0	\$0	\$120,000	\$0
<b>Total Non-Recurring Costs</b>	<b>\$0</b>	<b>\$388,000</b>	<b>\$582,000</b>	<b>\$725,000</b>	<b>\$1,549,000</b>
<b>2. Recurring Costs</b>					
<b>Personnel Salaries and Fringe Benefits</b>					
Legislative Resource Center (Forms Processing)	\$2,335,000	\$2,078,000	\$1,558,500	\$1,558,500	\$1,558,500
Legislative Computer Systems (Computer Support)	\$126,000	\$483,000	\$839,000	\$839,000	\$1,195,000
House Information Resources (Mainframe Support)	\$60,000	\$0	\$0	\$0	\$0
<b>Hardware (Lease and Maintenance)</b>					
Mainframe Costs	\$126,000	\$0	\$0	\$0	\$0
OSAR Optical Disc Storage Maintenance	\$134,000	\$0	\$0	\$0	\$0
Other Hardware Maintenance	\$2,000	\$11,000	\$22,000	\$29,000	\$29,000
Scanner License/Maintenance	\$107,000	\$0	\$0	\$0	\$0
New Scanner License/Maintenance	\$0	\$23,000	\$23,000	\$23,000	\$23,000
New Optical Disc Storage Maintenance	\$0	\$3,000	\$3,000	\$3,000	\$3,000
<b>Software (License and Maintenance)</b>					
Image System Software License/Maintenance	\$7,000	\$0	\$0	\$0	\$0
RS-6000 Servers License/Op Sys	\$34,000	\$0	\$0	\$0	\$0
Other Software License/Maintenance	\$47,000	\$26,000	\$69,000	\$69,000	\$69,000
PKI License/Maintenance	\$0	\$0	\$0	\$0	\$890,000
New Imaging System Maintenance	\$0	\$39,000	\$39,000	\$39,000	\$39,000
<b>External Vendor Services</b>					
PKI Vendor Hosting	\$0	\$0	\$0	\$305,000	\$0
<b>Total Recurring Costs</b>	<b>\$2,978,000</b>	<b>\$2,663,000</b>	<b>\$2,553,500</b>	<b>\$2,865,500</b>	<b>\$3,806,500</b>
<b>Total Estimated Costs</b>	<b>\$2,978,000</b>	<b>\$3,051,000</b>	<b>\$3,135,500</b>	<b>\$3,590,500</b>	<b>\$5,355,500</b>

Figure E.16: Sensitivity Analysis - Electronic vs. Hardcopy Submission Efficiency Gains

<sup>33</sup> Based on interviews with the Government of Canada, Lobby Registration Branch, efficiencies associated with the introduction of electronic filing capabilities amounted to approximately 50 percent reduction in staff processing resources. However, The Canadian Lobby Registration Branch received approximately 95 percent of submissions via electronic filing, primarily because a \$150 fee is charged to hard copy filers. To conservatively represent a scenario that the Clerk may experience, we assumed that a 25 percent reduction in forms processing staff would be appropriate.

A range of estimated reductions in LRC personnel salary and fringe benefit costs were also considered based on the corresponding percent of filers who submit FD and LDA forms electronically. For the purposes of this analysis, a straight-line decrease in LRC forms processing staff costs was assumed, proportional to the percentage of respondents who submit electronically. For example, 75 percent of filers submitting electronically would equate to a reduction of 37.5 percent decrease in LRC personnel costs. Figure 5.17: Sensitivity Analysis - Range of Electronic Filing Efficiency Gains on the following page represents the potential impact electronic filing submissions could have on the LRC forms processing staff costs.

Percent of Electronic Filers	100%	75%	50%	25%	0%
Estimated Reduction in LRC Personnel Costs <sup>34</sup>	50%	37.5%	25%	12.5%	0%
Total LRC Personnel Costs	\$1,039,000	\$1,319,530	\$1,558,500	\$1,818,250	\$2,078,000
Difference from Alternatives (Cost Savings)	\$1,039,000	\$758,470	\$519,500	\$259,750	\$0

*Figure 5.17: Sensitivity Analysis - Range of Electronic Filing Efficiency Gains*

### **5.3.2 Transition Cost Increases**

Cost information was gathered from vendors based on the high-level business needs associated with the four viable alternatives noted in this evaluation. However, these estimated costs may differ from actual implementation costs due to the specific vendor chosen and the detailed requirements of the alternative. Therefore, a scenario was developed to examine the impacts of significantly higher implementation costs on each alternative.

The total transition costs associated with the four alternatives were increased by 50 percent to represent a scenario in which the up-front costs to implement the alternatives are significantly more expensive. Although software integration/testing, hardware purchase and software purchase have the greatest likelihood for increase, to reflect the possible increases in all categories, the 50 percent factor was applied to the overall non-recurring charge for each alternative. Figure 5.18: Sensitivity Analysis - Transition Cost Increases on the following page demonstrates the impact of the cost increases on the alternatives.

---

<sup>34</sup> The Canadian Lobby Registration Branch experienced a 50 percent reduction in staff processing resources as a result of receiving 95 percent of submissions electronically. For the purposes of our analysis, we assumed 100 percent of submissions received electronically would equate to a 50 percent reduction in staff processing resources.

Cost Factor	Existing System	Alternative 1 Imaging/Workflow System	Alternative 2 Imaging/Workflow, w/Electronic Filing and Basic Encryption	Alternative 3 Imaging/Workflow, w/Electronic Filing, and PKI (Outsourced)	Alternative 4 Imaging/Workflow, w/Electronic Filing, and PKI (In-house)
<b>1. Non-Recurring Costs</b>					
Conversion/Testing	\$0	\$30,000	\$30,000	\$42,000	\$48,000
Software Integration/Customization	\$0	\$309,000	\$459,000	\$459,000	\$930,000
Hardware Purchase	\$0	\$115,500	\$142,500	\$160,500	\$160,500
Software Purchase	\$0	\$120,000	\$225,000	\$225,000	\$1,123,500
Training	\$0	\$7,500	\$16,500	\$21,000	\$61,500
CA Set-Up/Initialization	\$0	\$0	\$0	\$180,000	\$0
<b>Total Non-Recurring Costs</b>	<b>\$0</b>	<b>\$582,000</b>	<b>\$873,000</b>	<b>\$1,087,500</b>	<b>\$2,323,500</b>
<b>2. Recurring Costs</b>					
<b>Personnel Salaries and Fringe Benefits</b>					
Legislative Resource Center (Forms Processing)	\$2,335,000	\$2,078,000	\$2,078,000	\$2,078,000	\$2,078,000
Legislative Computer Systems (Computer Support)	\$126,000	\$483,000	\$839,000	\$839,000	\$1,195,000
House Information Resources (Mainframe Support)	\$60,000	\$0	\$0	\$0	\$0
<b>Hardware (Lease and Maintenance)</b>					
Mainframe Costs	\$126,000	\$0	\$0	\$0	\$0
OSAR Optical Disc Storage Maintenance	\$134,000	\$0	\$0	\$0	\$0
Other Hardware Maintenance	\$2,000	\$11,000	\$22,000	\$29,000	\$29,000
Scanner License/Maintenance	\$107,000	\$0	\$0	\$0	\$0
New Scanner License/Maintenance	\$0	\$23,000	\$23,000	\$23,000	\$23,000
New Optical Disc Storage Maintenance	\$0	\$3,000	\$3,000	\$3,000	\$3,000
<b>Software (License and Maintenance)</b>					
Image System Software License/Maintenance	\$7,000	\$0	\$0	\$0	\$0
RS-6000 Servers License/Op Sys	\$34,000	\$0	\$0	\$0	\$0
Other Software License/Maintenance	\$47,000	\$26,000	\$69,000	\$69,000	\$69,000
PKI License/Maintenance	\$0	\$0	\$0	\$0	\$890,000
New Imaging System Maintenance	\$0	\$39,000	\$39,000	\$39,000	\$39,000
<b>External Vendor Services</b>					
PKI Vendor Hosting	\$0	\$0	\$0	\$305,000	\$0
<b>Total Recurring Costs</b>	<b>\$2,978,000</b>	<b>\$2,663,000</b>	<b>\$3,073,000</b>	<b>\$3,385,000</b>	<b>\$4,326,000</b>
<b>Total Estimated Costs</b>	<b>\$2,978,000</b>	<b>\$3,245,000</b>	<b>\$3,946,000</b>	<b>\$4,472,500</b>	<b>\$6,649,500</b>

Figure 5.18: Sensitivity Analysis - Transition Cost Increases

## 5.4 Qualitative Analysis

In addition to the cost analysis and sensitivity analysis, an assessment of qualitative, or non-quantifiable, factors for the system alternatives was performed. The qualitative analysis was intended to provide additional evaluation criteria to analyze the alternatives.

Six qualitative factors were identified for use in analyzing the alternatives. A description of each of these factors is listed below.

- **Stakeholder Needs and Constraints** represent the extent to which each alternative satisfies the stakeholder needs and other constraints of the evaluation.
- **Management Control** represents the level of control that Clerk management has upon the outcomes, processes, schedules, and costs associated with an alternative.

- **Security Risk** represents the risks associated with application, network, and physical security for the implementation of an alternative.
- **Commercial Acceptance** represents the availability of knowledgeable customer support, upgrades, documentation, and proven success in the marketplace of an alternative.
- **Clerk Organizational Impact** represents the extent to which each alternative would impact the Clerk's business processes associated with the FD and LDA applications.
- **Filer Community Impact** represents the extent to which the FD/LDA respondent community is impacted by the alternative.

Figure 5.19: Overall Results of Qualitative Analysis on the following page presents an assessment of the qualitative factors for each alternative.



Qualitative Factor	Image/ Workflow System	Image/Workflow System, w/ Electronic Filing and Basic Encryption	Image/Workflow System, w/ Electronic Filing and an Outsourced PKI	Image/Workflow System, w/ Electronic Filing and an In-house PKI
<b>Stakeholder Needs and Constraints</b>	This alternative addresses some of the needs and constraints used for the evaluation. Specifically, the entire system is within the confines of the Clerk. However, this alternative does not address the need for electronic filing capabilities.	This alternative addresses all of the high-level business needs and constraints, but does not address the issue of non-repudiation associated with electronic filing.	This alternative addresses all the high-level business needs and constraints identified for the evaluation.	This alternative addresses all the high-level business needs and constraints identified for the evaluation.
<b>Management Control</b>	Due to the mature nature of the vendor markets associated with this alternative, the Clerk should have extensive management control over the outcomes, processes, schedule and costs.	Due to the mature nature of the vendor markets associated with this alternative, the Clerk should have extensive management control over the outcomes, processes, schedule and costs.	Although there are many different PKI outsource models available, all of them present the possibility that the Clerk would need to relinquish some control over the issuance of digital certificates to respondents. The impact on the Clerk's organization needs to be determined.	Over the next two years, the PKI market would experience enhanced pricing competition due to market entrants. This pricing competition would enhance the Clerk's ability for management control. <sup>35</sup>
<b>Security Risk</b>	This alternative should not introduce any new security risks.	With the introduction of electronic filing capabilities and technology components, some additional risks are introduced. New risks include risk of non-repudiation associated with filings and the protection of new technology components.	Using an outsourced PKI provider introduces the risk of security that would be present in an external vendor's environment. Although all PKI providers provide some level of security, assessing this risk component is sometimes difficult.	The technology components associated with this alternative allow for increased levels of confidentiality, data integrity and authentication. However, these technology components introduce additional risks associated with the protection of the technology components.

Figure 5.19: Overall Results of Qualitative Analysis.

<sup>35</sup> Based on "Pricing Public Key Infrastructure", September 8, 1998, Gartner Group.

Qualitative Factor	Image/ Workflow System	Image/Workflow System, w/ Electronic Filing and Basic Encryption	Image/Workflow System, w/ Electronic Filing and an Outsourced PKI	Image/Workflow System, w/ Electronic Filing and an In-house PKI
<b>Commercial Acceptance</b>	The functionality and technology components associated with this alternative have a wide commercial acceptance.	The functionality and technology components associated with this alternative have a wide commercial acceptance.	As additional vendors enter the PKI market over the next two years, the market would experience greater maturity and the technology would become more widely accepted and supported.	As additional vendors enter the PKI market over the next two years, the market would experience greater maturity and the technology would become more widely accepted and supported.
<b>Clerk Organizational Impact</b>	The current processing method used for the FD and LDA applications would be impacted by this alternative due to changes to a portion of the current business processes (i.e., scanning, indexing methods).	The functionality introduced by this alternative would have a far reaching impact on the Clerk’s organization due to the introduction of a new method for filers to submit FD and LDA forms.	The functionality introduced by this alternative would present new responsibilities for the Clerk’s Office. Other offices within the House could potentially utilize the technology associated with this alternative.	The functionality introduced by this alternative would present new responsibilities for the Clerk’s Office. Other offices within the House could potentially utilize the technology associated with this alternative.
<b>Filing Community Impact</b>	The LDA and FD respondent community would experience little impact as a result of this alternative.	The introduction of electronic filing functionality would present new filing capabilities for the FD and LDA respondent community.	The introduction of electronic filing functionality would present new filing capabilities for the FD and LDA respondent community. This alternative also introduces additional user identification procedures that may impact filers.	The introduction of electronic filing functionality would present new filing capabilities for the FD and LDA respondent community. This alternative also introduces additional user identification procedures that may impact filers.

Figure 5.19: Overall Results of Qualitative Analysis (continued)

JEFF TRANDAHL  
CLERK


H-154 THE CAPITOL

Office of the Clerk  
U.S. House of Representatives  
Washington, DC 20515-6601

MEMORANDUM

March 1, 1999

TO: John W. Lainhart, IV  
Inspector General

FROM: Jeff Trandahl   
Clerk of the House of Representatives

SUBJECT: Office of the Clerk's Comments to the Inspector General and  
PricewaterhouseCoopers Legislative Information Systems Evaluation

---

Thank you for the opportunity to comment on this draft Legislative Information Systems Evaluation. I have carefully reviewed the draft evaluation regarding the system options for replacing the Financial Disclosure (FD) and Lobby Disclosure Act (LDA) applications within the Office of the Clerk. I appreciate the time and effort that your office and the PwC team made in compiling this evaluation. I believe that the document establishes reasonable parameters for determining information technology solutions for the high-level business needs associated with the FD and LDA applications and recommends rational courses of action for using the results of the evaluation.

In general, I view the recommendations contained in this evaluation in two categories: those which are contingent upon the appropriateness of a particular alternative to the Clerk's business needs and those which may be addressed regardless of which alternative is pursued. Due to the breadth of the multiple alternatives presented in the evaluation, in many instances we did not deem a strict concur/not concur reply responsive to the recommendations. Therefore, some comments and commitments on the part of the Office of the Clerk to implement specific recommendations are subject to modification based upon further analysis and decisions which may affect the future course of this project.

I concur that the current system should be replaced as universally recommended in this audit. The following are my Office's specific comments from our analysis of the IG/PwC evaluation of the FD and LDA applications:

## FINDINGS AND RECOMMENDATIONS

### I. Response to Immediate Recommended Actions (pp. 12-13)

#### A.

**Finding:** Potential threats to the FD and LDA applications could be resolved with the implementation of security safeguards (Ex. 3, pp. 7-13 of 13).

**Recommendation:**

The Clerk should examine the recommended safeguards presented in the risk assessment to identify ones that can be implemented immediately to mitigate potential threats to the data and related assets of the FD and LDA applications.

**Response:** Concur with the general proposal of examining the recommended safeguards and implementing mitigating actions. Please see a more detailed response to the risk assessment findings and immediate recommended safeguards at Section III below.

#### B.

**Finding:** The success of implementing a new system would greatly depend on the individuals identified and dedicated to this project (p. 12).

**Recommendation:**

Organize a FD/LDA Project Team. A project manager should be assigned who would be directly responsible and accountable for the success of the project.

**Response:** The Clerk believes that this recommendation conforms with the Systems Development Life Cycle (SDLC) policies adopted by the House and should be followed for all projects of this magnitude. The Clerk could assign an in-house project manager. However, the Clerk's management staffing levels would not enable the organization to dedicate a full-time project manager to fulfill this recommendation. Similarly, the Clerk's staffing levels prevent full-time dedication of staff to the proposed project team. Therefore, the Clerk believes that the recommendation should include a proposal to contract with a vendor to assess the issues raised in this report, develop specifications for a request for proposal, and assist the project manager in overseeing installation of a replacement system. An in-house project manager and team would work with the vendor and be accountable for the success of the project.

C.

**Finding:** The success of managing and executing large-scale projects greatly relies on a sound work plan (p. 13).

**Recommendation:**

Develop a comprehensive work plan that allows the project manager to monitor progress and facilitate reporting to the Clerk and Committee on House Administration.

**Response:** Concur. This recommendation conforms with the SDLC policies.

D.

**Recommendation:**

In order to ensure the system solution and implementation resources can be procured in a timely manner, the Clerk's Office should develop a project budget (p. 13).

**Response:** Concur. The Clerk views the development of a project budget as a two-step process. First, costs associated with the development of a work plan by the project team, including vendor support to assist in devising detailed requirements and an RFP, will be identified. Next, long term costs associated with replacing the existing system will be identified after detailed requirements are developed by the project team. The long term costs will include costs associated with implementing and operating the selected system alternative.

**II. Response to System Planning, Development,  
and Implementation Recommended Actions (pp. 13-14)**

A.

**Recommendation:**

Conduct a Business Process Analysis to Determine the Benefits of OCR/ICR Technologies (p. 13).

**Response:** Concur. This analysis would be conducted by the FD/LDA project team. The Clerk will only pursue OCR/ICR technologies upon determination that the technology enables the Office to improve efficiencies in forms processing and will result in long-term cost savings.

**B.**

**Recommendation:**

Assess the Legal Implications and Acceptability of Electronic Filing prior to investing in this technology (p. 13).

**Response:** Concur. However, the Clerk believes that an analysis of the legal implications, including non repudiation, of electronic filing should be conducted under the auspices of the Committee on House Administration and the Office of the General Counsel. Such an analysis should only proceed upon determination that electronic filing is cost effective and appropriate based upon the volume of documents filed with the LRC.

**C.**

**Recommendation:**

Determine the use and acceptance of electronic filing by FD and LDA filers by surveying FD and LDA filers (p. 13).

**Response:** The Clerk is hesitant to survey FD and LDA filers to gauge acceptance and usage without confidence that cost effective electronic filing could be implemented. Such a survey would not be conducted without first determining the cost effectiveness, appropriateness, and, if necessary, non repudiation issues involved in electronic filing. As well, approval from CHA would be required prior to conducting such a survey.

**D.**

**Recommendation:**

Determine House-Wide Requirements for Public Key Infrastructure (p. 14).

**Response:** The Clerk believes that the assessment of House-wide needs for PKI technology should be determined in conjunction with the Committee on House Administration. The Clerk will share the findings of this report with CHA in an effort to further advance such electronic signature/filing programs in the House.

**E.**

**Recommendation:**

Make Decisions Regarding Implementation of Alternatives (p. 14).

**Response:** Concur. The Clerk views a decision regarding implementation of alternatives,

specifically the selection of the most cost-effective and practical alternative, as a decision which must be executed at the earliest possible time in order to ensure the success of the project.

F.

**Recommendation:**

Use the House SDLC Methodology (p. 14).

**Response:** Concur.

**III. Response to Risk Assessment findings and immediate recommended safeguards:**

**Findings:** The Risk Assessment section (Summary at p. 6 and Exhibit 3) of the evaluation identified nine (9) high-level potential threats and recommended one or more safeguards to mitigate the impact of these threats. Our comments to the risk assessment are as follows:

A.

**Threats:** Acts of nature, acts of terrorism, data center environmental compromise facilities, and hardware failure (Ex. 3, p. 5 of 13).

**Recommended Safeguard 1 (Ex. 3, pp. 7-9 of 13):**

Develop, test, and implement a BCP and document image backup procedure.

**Response:** LCS is participating in the joint development of a House-wide Business Continuity Contingency Plan (BCCP) in coordination with the CAO/HIR. When completed the plan will include a contingency for all computer-based systems of the Clerk.

**Recommended Safeguard 2 (Ex. 3, pp. 7-9 of 13):**

Use an off-site storage facility consistent with the practices of HIR, to store and maintain tape and/or image backups.

**Response:** In October 1998, LCS established an area of HB-1A in the Capitol building as an offsite storage area for FileNet indices. Backups are created on a daily, weekly, monthly and yearly basis. HIR implemented a corresponding tape backup for the mainframe data which corresponds to the FileNet indices. Optical Disks containing the FileNet transaction logs from April 1989 to November 1998 are stored in the Madison Building.

**Recommended Safeguard 3 (Ex. 3, p. 8 of 13):**

Strengthen physical access controls (e.g., implement card key, guest sign-in and double-door access).

**Response:** LCS has implemented a guest sign-in log for entry by visitors to room 2401 of the Longworth Building. In addition, an additional door alarm on the entryway to room 2403 was provided by the Physical Security Branch of the Capitol Police. Signs have been placed above the door to 2403 and all staff keys were collected as well. Finally, LCS submitted a request to the Office of the Architect of the Capitol for installation of other physical security equipment, including an upgraded alarm system with proximity card key entry.

**B.**

**Threats:** Intentional acts by House staff or human error by staff and logical/physical penetration to data center by unauthorized public users (Ex. 3, p. 5 of 13).

**Recommended Safeguards 1 and 2 (Ex. 3, pp. 9-12 of 13):**

Grant access to users based upon job duties and provide for segregation of duties through workflow functionality. Appoint a security officer to monitor and manage security.

**Response:** The Clerk will ensure that user access is based upon job duties and that workflow functionality issues are addressed during replacement of the current system. In 1995, LCS appointed a Clerk/LCS LAN security staff member and in 1998, an additional LCS staff member assumed application system and physical access security responsibilities.

**Recommended Safeguard 3 (Ex. 3, p. 11 of 13):**

Improve application change control procedures using change control tools.

**Response:** LRC and LCS staff will improve the formal documentation of all application and system software changes. Currently, these changes are approved in advance and fully tested by LRC and LCS staff before production implementation.

**C.**

**Threat:** Misrepresentation of identity of public users (Ex. 3, p. 5 of 13).

**Recommended Safeguard (Ex. 3, p. 10 of 13):**

Implement manual or automated authentication procedures that are consistent with the spirit of the EIGA and LDA.

**Response:** The Clerk concurs that the potential for the misrepresentation of the identity of



public users with respect to the FD application exists. The LRC could implement a photo identification check in the Public Information Section to authenticate the accuracy of the information entered in the automated fields during logon to the FD application. The LDA does not require identification or authentication.