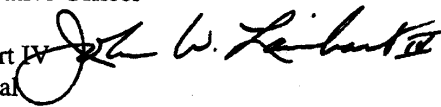


John W. Lainhart IV
Inspector General

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

MEMORANDUM

TO: Scot M. Faulkner
Chief Administrative Officer

FROM: John W. Lainhart IV 
Inspector General

DATE: July 18, 1995

SUBJECT: Audit Report - The House Needs To Follow A Structured Approach For Managing
And Controlling System Development Life Cycle Activities Of Its Computer
Systems (Report No. 95-CAO-20)

This is our final draft report on system development life cycle activities within the House. The objective of the audit were to review and evaluate: (1) the effectiveness of systems development standards, policies, procedures, and system development methodologies; (2) roles and responsibilities of system development personnel; and (3) the quality of systems development documentation. In this report, we identified problems and made recommendations for corrective actions.

In response to our June 26, 1995 draft report, your office fully concurred with our findings and recommendations. The formal management response provided by your office was incorporated in this final report and included in its entirety as an appendix. The corrective actions taken and planned by your office is appropriate and, when fully implemented, should adequately respond to the recommendations.

We appreciate your office's positive response and concurrence with the recommendations, and 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 Craig W. Silverthorne at (202) 226-1250.

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

**THE HOUSE NEEDS TO FOLLOW A STRUCTURED APPROACH
FOR MANAGING AND CONTROLLING SYSTEM DEVELOPMENT LIFE CYCLE
ACTIVITIES OF ITS COMPUTER SYSTEMS**

*Report No. 95-CAO-20
July 18, 1995*

RESULTS IN BRIEF

CONCLUSIONS

Computer systems developed at the House were not guided by a formal methodology. Without such a methodology the system development activities resulted in systems that did not meet user needs and were not cost-effective. Neither the Committee on House Administration nor House Information Systems (HIS¹) management mandated the use of a formal Systems Development Life Cycle (SDLC) methodology for HIS system development and maintenance efforts. Federal government and private sector best practices for systems development efforts require the use of a formal SDLC in order to minimize the risks associated with developing, purchasing, maintaining, and implementing systems.

The House developed, implemented, and continued to maintain numerous system solutions in-house, when comparable and less expensive systems may have been available commercially. For example, features similar to those of the in-house developed Integrated Systems and Information Services (ISIS) and Member Information Network (MIN) systems (which are legislative and news search and retrieval systems) are available in vendor solutions such as LEXIS/NEXIS and Legislate. The features of Micromin, which is an in-house developed Correspondence Management System (CMS), are available in at least 10 other vendor systems. Federal government regulations require the consideration of commercially available off-the-shelf systems during SDLC efforts.

¹On June 14, 1995, HIS was renamed by the Committee on House Oversight and is now House Information Resources (HIR).

RECOMMENDATIONS

We recommend that the Chief Administrative Officer direct the Associate Administrator of HIR to: (1) adopt a formal SDLC methodology that meets the requirements of the National Institute of Standards and Technology's FIPS Publications and Special Publication 500-153 for all system development efforts; (2) adhere to Federal government guidelines and use commercial software packages in lieu of in-house systems whenever cost-beneficial; and (3) perform a cost-benefit analysis to determine whether existing HIR systems that compete with commercially available off-the-shelf packages should continue to be maintained by HIR, and if not present a migration plan to the Committee on House Oversight.

MANAGEMENT RESPONSE

On July 11, 1995, the Office of the CAO fully concurred with the findings and recommendations in this report. As part of their system of continuous improvement, the CAO indicated that HIR will implement control mechanisms to insure that system development, maintenance, and operations will be performed in a businesslike manner. This will be achieved primarily through the implementation of an appropriate SDLC methodology and through the restructuring of HIR and the consolidation of all application and database activity. Furthermore, HIR has designated the Integration Group to be responsible for application system organization and will adopt the recommendation to buy commercial software packages rather than build software packages. Also, as part of the Office 2000 initiative, HIR will re-evaluate all the information retrieval systems and, as a result of the evaluation, decisions to phase out existing in-house developed systems will be presented to the Committee on House Oversight routinely for approval.

OFFICE OF INSPECTOR GENERAL COMMENTS

The CAO current and planned actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

TABLE OF CONTENTS

TRANSMITTAL MEMORANDUM

RESULTS IN BRIEF i

I. INTRODUCTION

 Background 1

 Objectives, Scope, And Methodology 2

 Internal Controls 4

 Prior Audit Coverage 4

II. FINDINGS AND RECOMMENDATIONS

 Finding A: The House Did Not Develop Computer Systems Using A Formal
 Systems Development Life Cycle (SDLC) Methodology 6

 Finding B: Existing In-House Systems Should Be Considered For Replacement
 By Commercially Available Solutions 10

III. EXHIBITS

 Exhibit A: SDLC Phases 12

 Exhibit B: Roles And Responsibilities 13

 Exhibit C: Project Documentation 15

 Exhibit D: HIS Project Documentation Comparison 18

IV. APPENDIX

 Appendix: CAO Management Reponse To The Draft Report 19

I. INTRODUCTION

Background

House Information Systems' (HIS¹) mission is to "satisfy the requirements for information, information technology, and related computer service of the Members, committees and staff of the U.S. House of Representatives." HIS is the major provider of information technology services to the House and is responsible for the technical infrastructure and other services. It helps to shape the House information technology infrastructure by matching office needs with vendor and custom developed products and services.

The House information systems environment consists of a wide range of technologies:

- IBM mainframe;
- Mainframe communications to terminals;
- Local area networks (LANs);
- Wide area networks (WANs)
- Internet² access;
- Microcomputers; and
- Minicomputers.

HIS provides varying levels of support for each of these technologies. Office level systems within the House environment are not under the direct control of HIS and, therefore, are independent with respect to adherence to HIS standards and guidelines. These office-level systems include LANs, stand-alone personal computers, and other departmental systems. These systems may reside in Member (Washington, D.C. and district), committee, or other House offices, and are supported by outside vendors who install and maintain the office-level systems. HIS or internal office personnel also maintain these office-level systems.

¹On June 14, 1995, HIS was renamed by the Committee on House Oversight and is now House Information Resources (HIR).

²The Internet is a large international network that connects many computer systems, providing network services, including electronic mail (i.e., e-mail), remote terminal sessions, and multi-media services such as the world-wide web.

During the audit period, HIS was organized into the following six divisions: Administrative Systems (AS); Communication Services; Computer Center; Customer Services Group; Information Resource Systems (IRS); and Customer Applications Group (CAG).

Objectives, Scope, And Methodology

The performance audits conducted as part of the overall assessment of the House included a comprehensive review of HIS operations and the House information systems environment. The objectives of this audit of HIS' systems development practices were to review and evaluate:

- The effectiveness of systems development standards, policies, procedures and systems development methodologies;
- Roles and responsibilities of system development personnel; and
- The quality of systems development documentation.

The scope of the audit included review of procedures in place for the three major systems development groups within HIS: AS, IRS, and CAG. In performing our review we also considered the following factors especially as they related to the economy, efficiency, and effectiveness of the systems development process:

- Technology architecture;
- Development of in-house systems versus commercial off-the-shelf systems;
- The development and support of multiple systems that perform similar functions;
- Organizational issues (e.g., steering committee); and
- U.S. House of Representatives Customer Satisfaction Survey.

We conducted our review in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Our review was based on the organizational structure, plans, standards, policies, and procedures in place as of December 31, 1994. Our field work for this review was performed during February through May 1995. In conducting our review, we performed the following specific tasks:

- Gathered documentation and conducted interviews.

- Identified business objectives and control techniques consistent with sound systems development standards based on current industry standards.
- Gained an understanding of the internal control environment surrounding the systems development process.
- Assessed the risks surrounding systems development and developed a preliminary risk assessment of the review areas.
- Developed and executed detailed testing procedures to address the review areas identified by our risk assessment.

Our primary techniques for gathering and verifying data were through interviews with key personnel and the evaluation of systems documentation and other material provided to us by HIS and other House offices. Price Waterhouse LLP Computerized Information System (CIS) Audit specialists assisted in the execution of the review tasks and detailed testing.

We also applied information systems audit guidelines used at Federal government and private industry computer installations in managing and controlling the design, development, and modification of computer systems. These guidelines and standards are described in government and private industry publications, such as:

- National Institute of Standards and Technology (NIST) - Federal Information Processing Standards (FIPS) Publications
- NIST Special Publication 500-153 - Guide to Auditing for Controls and Security: A System Development Life Cycle Approach
- Office of Management and Budget (OMB) Circulars:
 - A-127, Financial Management Systems
 - A-130, Management of Federal Information Resources
 - A-134, Financial Accounting Principals and Standards
- Institute of Internal Auditors - Systems Auditability and Control (SAC) Report
- Information Systems Audit and Control Foundation - Computerized Information Systems (CIS) Audit Manual
- Price Waterhouse LLP Systems Management Methodology (SMM), Strategic Information Systems Planning, System Development, Package Implementation, Information Systems Risk Management and Disaster Contingency Planning modules

Although the House is not mandated to comply with the standards used in our review, they represent sound practices that other government agencies and private industry follow.

Internal Controls

This review evaluated internal controls related to HIS' system development process, in general, and specifically evaluated projects including the Financial Management System (FMS), Daily Digest, Integrated Systems and Information Services (ISIS), Member Information Network (MIN), and Micromin. It discusses significant internal control weaknesses identified in HIS' system development processes.

Prior Audit Coverage

As part of a comprehensive review of HIS operations, we are preparing a series of reports addressing weaknesses associated with the House information systems environment. The results of three completed projects are summarized below:

Internet Security Weaknesses (Report No. 95-CAO-03): This report noted serious weaknesses surrounding access to the House network and Member office systems via the Internet through external agencies on CapNet³. The report identified the capability for unauthorized individuals to access Member systems and read mail in a Member's correspondence management system. For example, we were able to read a Member's mail and other data, and send an e-mail message to the Inspector General's office posing as that Member. In this case we exploited a "back door" into the House network, and, thereby, Member offices, and easily and effectively bypassed the HIS firewall⁴ installed to protect the HIS "front door" into the network. The report contained nine recommendations to correct the internal control weaknesses and to prevent recurrence. HIS agreed to correct the deficiencies we identified and is taking actions to correct them.

Proposed New Financial Management System Will Not Meet the House's Needs And Should Be Terminated (Report No. 95-CAO-02): This review evaluated the functional adequacy of the proposed FMS and the system development life cycle procedures that were utilized in the development of the system. This report recommended that the system be terminated and also made recommendations to improve the systems development practices within HIS as well as provide better management oversight. The Chief Administrative Officer agreed to terminate the new FMS system and to make the management improvements recommended, and is taking actions to correct the deficiencies identified.

³CapNet is the internal network connecting the various Legislative Branch agencies, including the House.

⁴A firewall is a combination of computer hardware and software designed to control the flow of information between an organization's internal systems and systems outside the organization.

Information Systems Security Weaknesses (Report No. 95-CAO-01): This report noted serious weaknesses surrounding remote dial-in access to House office-level systems. The report identified the capability for unauthorized individuals to access Member systems and read mail in a Member's correspondence management system. The report also identified the capability to change outgoing correspondence in a Member's system to alter the position of the Member on a sensitive issue. Collectively, these weaknesses highlight the risks associated with dial-in access and the need for improved security to reduce the risk of access to sensitive House computer resources by unauthorized individuals. The report contained seven recommendations to correct the internal control weaknesses and to prevent recurrence. HIS agreed to correct the deficiencies we identified and is taking actions to correct them.

In addition, a management advisory services study was performed for HIS as described below:

Arthur Andersen & Co. (AA) Report - Technical Design of the new FMS, May 1987: This review evaluated the design of the new FMS including file and software design, control and security procedures to guard against unauthorized access and system audit trails, accounting checkpoints, and recovery mechanisms. This report validated the technical approach, but recommended that file structure changes be implemented to improve performance. AA also recommended HIS document all known control requirements for the system.

II. FINDINGS AND RECOMMENDATIONS

Finding A: The House Did Not Develop Computer Systems Using A Formal Systems Development Life Cycle (SDLC) Methodology

Computer systems developed at the House were not guided by a formal methodology. Without such a methodology the system development activities resulted in systems that did not meet user needs and were not cost-effective. Neither the Committee on House Administration nor HIS management mandated the use of a formal SDLC methodology for HIS system development and maintenance efforts. Federal government and private sector best practices for systems development efforts require the use of a formal SDLC in order to minimize the risks associated with developing, purchasing, maintaining and implementing systems.

A standard approach to SDLC, with well defined, action oriented phases, should be established to provide an effective mechanism for controlling projects under development. This approach must provide review points that enable managers to continually monitor and assess progress, performance, and budget status and, where necessary, reevaluate, reschedule, or terminate development work. Therefore, the SDLC approach should encompass periodic reporting to management. Problems encountered should be discussed and resolved. Each phase must be completed before the next can be started. At the completion of each phase, all previous work is reviewed, and a "go/no go" decision is made. This progression provides a structured approach to the development process. The technique is as applicable during initial system design as it is during the modification process; and it is also as applicable during the acquisition of off-the-shelf packages, use of prototyping, use of contractors, and end-user computing. See Exhibit A for a short description of each SDLC phase.

SDLC methodology defines specific responsibilities for project participants and promotes responsible communication among programmers, systems analysts, quality assurance personnel, users, project manager, and the project steering committee. Responsibilities and duties are established at the outset of the project and provide for performance and management accountability. Management control of the project is ensured by formally assigning responsibilities. See Exhibit B for additional details on project participant roles and responsibilities.

Documentation is the process of describing on paper how a CIS operates. Good documentation has the following uses:

- Provides management with a clear understanding of system objectives, concepts, and outputs and indicates whether SDLC policies are being adhered to.
- Ensures correct and efficient processing within both data processing and user areas.

- Provides a convenient reference for systems analysts and programmers responsible for maintaining existing systems and programs.
- Provides a primary base for training.
- Serves as a basis for review of internal controls.

See Exhibit C for additional details on required project documentation.

HIS has three separate departments that perform systems development and maintenance activities within the House information systems environment. These three departments are AS, IRS, and CAG. We tested four system development projects--FMS and Daily Digest (both AS projects), ISIS (an IRS project), and Micromin (a CAG project)--for the completion of 22 key project documents. We found that many project documents were either missing or incomplete for each of the projects. For example, each of the projects were missing 5 to 16 key project documents and also had 2 to 9 incomplete documents. (See Exhibit D.)

The lack of a formal SDLC resulted in the following:

- Systems developed without defining requirements;
- Systems developed in-house when packaged (off-the-shelf) solutions may have been available;
- Systems not adequately tested prior to production use;
- Inadequate project planning and tracking;
- Inadequate systems documentation;
- User workflows not reviewed in developing functional requirements;
- No empowered group to represent all user offices;
- No security analysis performed; and
- Inadequate training plans.

In addition, the lack of a formal SDLC and inadequate informal system development practices resulted in the following:

- Systems that did not meet House needs;
- Budget and schedule overruns;
- Projects that were never completed; and
- Duplicate systems.

These weaknesses were evident in projects such as the FMS. This SDLC effort was not completed after nine years and an investment of \$5 million. In addition, the project lacked sufficient project planning and tracking, alternatives analyses, consideration of user workflows, testing and requirements definition. Furthermore, we recently reported that the proposed system would not meet the House's needs for financial management, and should be terminated. Management agreed with our recommendation and terminated the project. (See Report No. 95-CAO-02.)

In addition, ISIS and MIN are HIS supported systems that provide an access path to various legislative and news databases. MIN is a mainframe application, using older technology and, therefore, its features are not as robust as those available with current client/server based technology. The ISIS project was initiated in 1989 to replace MIN with a client/server based solution. However, after 6 years (and about 4 years after the first operational release of ISIS was available) MIN still has about 4,500 users compared to about 500 ISIS users.

We also found that in many cases roles and responsibilities of project participants were inadequate. For example, there were no project steering committees in place to make "go no/go" decisions at the end of each phase of the project and in the FMS, user representation and project tracking by the project manager was often lacking. In addition, for the ISIS project, user representatives were not empowered to represent the entire user community.

In summary, systems development and maintenance guidelines, procedures, and work products were informal, and HIS followed ad hoc procedures that were inadequate; users needed to be involved and management needed to carefully monitor system projects. Furthermore, documentation was often non-existent or incomplete. A structured SDLC methodology will provide such a framework for successful management and control.

Recommendation

We recommend that the Chief Administrative Officer direct the Associate Administrator of HIR to adopt a formal SDLC methodology that meets the requirements of NIST's FIPS Publications and Special Publication 500-153 for all system development efforts.

Management Response

On July 11, 1995, the Director of Internal Controls and Continuous Improvement, on behalf of the CAO, fully concurred with this finding and recommendation (see Appendix). As part of their system of continuous improvement, the response indicated that House Information Resources (HIR) will implement control mechanisms to insure that system development, maintenance, and operations will be performed in a businesslike manner. This will be achieved primarily through the implementation of an appropriate System Development Life Cycle (SDLC) methodology and through the restructuring of HIR and the consolidation of all application and database activity.

Office of Inspector General Comments

The CAO current and planned actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Finding B: Existing In-House Systems Should Be Considered For Replacement by Commercially Available Solutions

The House developed, implemented, and continued to maintain numerous system solutions in-house, when comparable and less expensive systems may have been available commercially. For example, features similar to those of the in-house developed ISIS and MIN systems (which are legislative and news search and retrieval systems) are available in vendor solutions such as LEXIS/NEXIS and Legislate. The features of Micromin, which was an in-house developed CMS, were available in at least 10 other vendor systems. Federal government regulations require the consideration of commercially available off-the-shelf systems during SDLC efforts.

ISIS and MIN provide members, Committees, and staff with news and legislative search and retrieval capabilities. ISIS utilizes client/server technology while MIN is mainframe based. For the most part, data that is provided by these in-house developed systems can be found in existing and proven commercial products such as LEXIS/NEXIS and Legislate. Although HIS has performed a high level analysis of the capability of these products against services provided in-house, no formal, detailed analysis of these outside services against a comprehensive set of House requirements has been made nor has a cost-benefit analysis been performed to determine if in-house maintenance of ISIS and MIN should be continued.

In addition, at least 11 different CMS applications were in use at the House during the audit period. All of these packages were commercial off-the-shelf packages except for Micromin which was developed and is being maintained by HIS. According to available inventory records, approximately 21 percent of the user community uses Micromin, while 79 percent uses a vendor solution. According to the recent customer satisfaction survey, the level of user satisfaction among the different packages is comparable, indicating that a vendor based solution for the Micromin users group is feasible. The use of an in-house CMS application when vendor based solutions are available may not be warranted, and result in inefficient utilization of HIS resources and unnecessary development and support costs.

Recommendations

We recommend that the Chief Administrative Officer:

1. Adhere to Federal government guidelines and use commercial software packages in lieu of in-house systems whenever cost-beneficial; and
2. Perform a cost-benefit analysis to determine whether existing HIS systems that compete with commercially available off-the-shelf packages should continue to be maintained by HIS, and if not, present a migration plan to the Committee on House Oversight.

Management Response

On July 11, 1995, the Director of Internal Controls and Continuous Improvement, on behalf of the CAO, fully concurred with this finding and recommendation (see Appendix). The response indicated that House Information Resources (HIR) will designate the Integration Group to be responsible for application system organization and will adopt the recommendation to buy commercial software packages rather than build software packages. Also, as part of the Office 2000 initiative, HIR will re-evaluate all the information retrieval systems and, as a result of the evaluation, decisions to phase out existing in-house developed systems will be presented to the Committee on House Oversight routinely for approval.

Office of Inspector General Comments

The CAO current and planned actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Exhibit A

SDLC Phases

SDLC PHASE	DESCRIPTION
I. Project Initiation	During this phase the business need is established and validated and alternative options to satisfy the need are recommended and approved. This phase should also include a cost/benefit analysis of each alternative and a final recommendation.
II. Project Definition	In this phase the functional requirements of the system are defined, and detailed project planning commences. This phase should also identify initial internal control and security requirements.
III. System Design	The purpose of this phase is to identify a specification for the proposed solution. The detailed design specifications describe the physical solution in a way that allows for coding with little additional analysis.
IV. Programming and Training	This phase results in programs which are ready for testing, evaluation, certification and accreditation, and installation.
V. Evaluation and Acceptance	In this phase, integration and system testing occurs. In order to validate the systems functions, test data is used and the system is field tested at operational sites.
VI. Installation and Operation	The purpose of this phase is to implement the approved operational plan, including extension/installation at other sites and continue approved operations.
VII. Maintenance	This phase addresses the monitoring and controlling of modifications to the system after it becomes operational.
VIII. Post-Implementation Review	This final phase provides for a comprehensive review of the system after it has been implemented and operational for a minimum of 6 months.

Exhibit B

Roles and Responsibilities

PROJECT PARTICIPANT	RESPONSIBILITY
Project Steering Committee	To ensure top management control during the entire course of the SDLC, a project steering committee should be formed to regularly oversee and review progress, and make decisions at each critical stage. The committee should decide whether to initiate, continue, revise, or terminate the project and should consider any strategic matters affecting the project, provide overall direction, and establish both accountability and primary management controls. The committee should meet regularly to review and analyze progress and performance, and to approve completed work and plans for the next phase before the project proceeds.
User	These individuals are responsible for identifying the business need for a new system or major enhancement. The User should identify alternative solutions for the need and determine the feasibility and cost/benefit of the various alternatives. The User also is responsible for conducting a risk analysis to assess the potential vulnerabilities of the system or application being developed. The Sponsor/User is ultimately responsible for the "go/no go" decision for the systems and should provide approvals at the end of each phase of the life cycle. These individuals should have the skills necessary to identify functional requirements and prepare comprehensive acceptance test cases. The User must be empowered to represent the user community.
Project Manager	The Project Manager is responsible for seeing that the system is properly designed to meet the user's requirements and that the project adheres to an appropriate schedule. The Project Manager has overall responsibility for ensuring that all documentation is prepared as the system progresses through the SDLC phases. The Project Manager is accountable to the User and the project steering committee.
Systems Analyst	The Systems Analyst is responsible for analyzing user requirements and determining the approach for systems design.

Programmer	The programmer is responsible for the coding and initial unit and systems testing.
Quality Assurance (QA) Specialist	The QA staff is responsible for assuring the User that the application system is developed in accordance with the system's stated objectives, contains required internal controls and security to produce accurate results on a consistent basis, and operates in conformance with requirements and data processing procedures.
Contracting Officer	When contracting with vendors to provide part or all of the system development activity, this individual is responsible for awarding and managing contracts. The Contracting Officer is responsible for ensuring that the vendor or contractor complies with the terms of the contract.

Exhibit C

Project Documentation

SDLC Phase	Documentation	Description
PROJECT INITIATION	Needs Statement	Deficiencies in existing capabilities, new or changed program requirements, or opportunities for increased economy and efficiency. Should also contain justification for exploring alternative solutions for the deficiencies.
	Feasibility Study	Provides an analysis of the objectives, requirements and system concepts, an evaluation of alternative approaches and identification of a proposed approach.
	Risk Analysis	Identifies internal control and security vulnerabilities of the system
	Cost/Benefit Analysis	Provides project team with cost/benefit information, including the impact of security and internal control requirements on the information.
	System Decision Paper**	Provides information critical to the decision making process during the SDLC. It contains business need, milestones, thresholds, issues and risks, alternatives, cost/benefit, management plan, supporting rationale for decisions, project cost and decisions made by the IRM.
PROJECT DEFINITION	Project Plan**	Specifies the strategy for managing the project. It defines goals and activities for each phase
	Functional Requirements	Provides a basis for a common understanding between users and designers on the initial definition of the application.

	Data Requirements Input Layout Record Layout Report Layout Output Product Distribution List	Data descriptions and technical information about data collection requirements
SYSTEM DESIGN	System Specifications System Flowchart	Describes for analysts the requirements, operating environment, design characteristics and program specifications for the system
	Program Specifications	Describes for programmers, the requirements, operating environment and design characteristics of computer programs.
	Database Specifications	Describes the nature, logic and physical characteristics of a particular data base.
	Security Plan	Security specifications to meet functional security requirements.
	Validation, Verification and Testing Plan**	Plan for the evaluation of quality and correctness of software, including requirements and design documentation. Also provides plans for testing of software.
PROGRAMMING & TRAINING	User manual**	Description of the functions of the software in non-computer terminology for the benefit of the user.

	Operations/Maintenance manual**	<p>The Operations manual provide computer operations with a description of the software and the operating environment so that the software can be run.</p> <p>The Maintenance manual provides programmers with information and source code necessary to understand the system, operating environment and maintenance procedures and security requirements.</p>
	Installation and Conversion Plan**	A tool for managing the installation or implementation of a system at various locations.
EVALUATION AND ACCEPTANCE	Test Analysis & Security Evaluation Report	This document is used to document the test analysis results and findings, present the demonstrated capabilities and deficiencies, and provide a basis for preparing a statement of system readiness.

** - These documents are updated during all subsequent phases.

Exhibit D

HIS Project Documentation Comparison

	FMS	ISIS	MICROMIN	DAILY DIGEST
Project Request Documentation	Inc		•	Inc
Feasibility Study		Inc	Inc	N/A
Risk Analysis				
Cost/Benefit Analysis			Inc	
Project Plan	Inc	•		Inc
Functional Requirements	Inc	•	•	Inc
Data Requirements	Inc	•	•	
System/Subsystem Specifications	Inc	•	•	
Program Specifications	•	•	•	Inc
Database Specifications	•	•	•	
Security Plan	Inc	•		
Validation, Verification, and Testing Plan and Specifications	Inc	Inc		
User Manuals	•	•	•	
Operations/Maintenance Manuals	•	•	•	
Installation and Conversion Plan	Inc		•	N/A
Test Analysis and Security Evaluation Report	Inc	•		
System Decision Papers				
Output Product Distribution List		N/A		
System Flowchart	•	•	•	
Input Layouts	•	•	•	
Record Layouts	•	•	•	
Report Layouts	•	•		

Legend

• Adequate Level of Documentation

Inc Document Provided but Incomplete


N/A Document Not Applicable to Project

A blank cell indicates no evidence provided that document existed.

Office of the
Chief Administrative Officer
U.S. House of Representatives
Washington, DC 20515-6860

MEMORANDUM

TO: Robert B. Frey III
Deputy Inspector General

FROM: Thomas J. Simon 
Director of Internal Controls and Continuous Improvement

DATE: July 11, 1995

SUBJECT: Draft Audit Report - Systems Development Life Cycle

We appreciate the opportunity to comment on your draft report. We deeply appreciate your efforts and are in general agreement with the findings and recommendations. Specific comments on each recommendation follow. If there are any questions or additional information required regarding this reply, please contact me at (202) 226-1854.

Finding A

Recommendation: HIR is in the process of implementing this recommendation with a number of control mechanisms to insure that system development, maintenance and operations are conducted in an efficient businesslike manner. Implementation of appropriate System Development Life Cycle methodology will be an integral part of this reform. The SDLC steps outlined in the findings are well-understood and will be implemented and tailored to the situation. The restructuring of HIR and the consolidation of all application and database activity will facilitate the implementation of this recommendation.

Finding B

Recommendation 1: HIR has fully adopted the recommendation to "buy" rather than "build" and has demonstrated its policy in this area by designating its application system organization as the Integration Group.

Recommendation 2: HIR is in the process of re-evaluating all its information retrieval offerings as part of its Office 2000 initiative. Existing in-house developed systems will be phased out as economically feasible and in a manner that minimizes hardship to Members. Individual decisions will be presented to the Committee on House Oversight on a regular basis.