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

MEMORANDUM

TO: The Honorable Bill Thomas, Chairman
Committee on House Administration

The Honorable Steny Hoyer, Ranking Minority Member
Committee on House Administration

FROM: Robert B. Frey III
Deputy Inspector General

DATE: December 21, 1999

SUBJECT: Audit Report -- Summary of the House Year 2000 Efforts
(Report No. 99-CAO-10)

This is our final audit report on our review of the Year 2000 (Y2K) readiness of the U.S. House of Representatives (House). The primary objective of this audit was to assess the effectiveness of the Members' offices, Clerk, Sergeant At Arms (SAA), and Chief Administrative Officer (CAO) compliance with the validation/testing and implementation phases of the House Y2K plan. To accomplish these audit objectives, we assessed the unit, integration, acceptance and end-to-end Y2K testing in the offices of the Clerk, SAA, and CAO; the CAO's assistance to Members and Committees in preparing for Y2K; and the CAO's Business Continuity and Contingency planning for the House. We reviewed testing in detail because thorough testing is needed to ensure that the work done in the prior phases adequately prepared the House to meet the Y2K challenges.

In this audit we discuss actions taken by the House to minimize the risk of Y2K date related failures in House systems.

Should you have any questions or require additional information regarding this review, I am available at your convenience.

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

SUMMARY OF THE HOUSE YEAR 2000 EFFORTS

I. INTRODUCTION

Background

The Year 2000 (Y2K) date change is one of the most significant changes ever faced by the Information Technology industry. It will have an enormous impact on business applications and system software, potentially even putting some companies out of business. The date change has the potential to cripple an organization's ability to execute its critical business functions. It impacts everything from payroll and pension calculations to budgeting to electronic data transfers. Failures can include programs ending abnormally or, worse, returning incorrect results. Even applications that do not use dates are at risk, as they may depend on others that do. It is estimated that companies in the United States will spend billions of dollars addressing the software changes required by the coming millennium. What makes this problem so daunting is its magnitude, not its technical complexity. The Y2K initiative has a deadline that cannot be extended.

The biggest challenges to be faced by the U.S. House of Representatives (House) are keeping tight project control of the Y2K effort in its final phases and securing active House-wide participation with the contingency planning process. Members and Committee offices are responsible, in conjunction with HIR, for updating their computers in preparation for Y2K. The Clerk, Sergeant At Arms (SAA), and Chief Administrative Officer (CAO), are responsible to the Committee on House Administration for the successful implementation of Y2K compliant information technology assets; i.e., mission critical and other essential computer systems. The GAO *Year 2000 Computing Crisis: An Assessment Guide*, separated Y2K issues into five phases; awareness, assessment, renovation, validation/testing and implementation. Each of these phases can be broken down into individual tasks. Prior audits have shown that House Y2K Plans adequately addressed the first three of the five generally accepted phases recommended by the GAO to effectively plan, manage and evaluate Y2K projects. This audit addresses the last two phases, validating/testing and implementation, critical to the successful transition of House computer systems into the year 2000.

As criteria for testing, the CAO adopted the General Accounting Office (GAO) *Year 2000 Computing Crisis: A Testing Guide*. The guide describes key processes for effectively designing, conducting, and reporting test results. The testing process consists of several tasks (i.e., unit, software integration, systems acceptance, and end-to-end testing) performed in a sequential order of increasingly more complex levels of testing. Unit testing is performed to verify that individual software subprograms, subroutines, or procedures work as intended. Software integration testing verifies that units of software, whether subprograms, programs, or applications, work together as intended after they successfully pass unit testing. System acceptance testing is performed by and for users to determine that the complete system, consisting of the renovated software program, target hardware, and systems software, satisfies the users' functional, performance, and security requirements. Finally, end-to-end testing verifies that a defined set of interrelated systems operate as intended in a live production environment. Successful testing at the more complex levels is dependent upon complete testing

at the lower levels. For example, unless interfacing systems have been thoroughly tested on their own, it would be much more difficult to isolate and correct errors that occur in end-to-end testing of several systems simultaneously.

Concurrent with this testing effort, the CAO continued development of Business Continuity and Contingency Plans (BCCP) seeking House-wide participation using the GAO's *Year 2000 Computing Crisis: Business Continuity and Contingency Planning Guide* as criteria. The guide describes four phases for reducing the risk and potential impact of Y2K induced information system failures on core business processes. The first phase, Initiation, involves establishing a business continuity project work group, strategy, and master schedule. The second phase, Business Impact Analysis, assesses the potential impact of mission critical system failures. The third phase, Contingency Planning, identifies contingency plans and implementation modes and triggers, develops a "zero day" strategy and procedures for the period between December 30, 1999, and January 3, 2000, and establishes business resumption teams. The final phase, Testing, validates the business continuity strategy.

Objectives, Scope and Methodology

This audit focused on the Y2K plans and processes used to perform validation and testing of those systems renovated as part of the House Y2K program. The primary objective of this audit was to assess the effectiveness of the Members offices, Clerk, SAA, and CAO compliance with the validation/testing and implementation phases of the House Y2K plan. We evaluated whether the Officers had appointed project leaders, assigned personnel to work on the initiative, prepared and executed test plans, prioritized work for mission critical projects, and established target dates. To accomplish our objectives, we performed a detailed review of the CAO's unit, integration, acceptance, and end-to-end Y2K compliance validation/testing and a limited review of the Clerk's and SAA's Y2K testing efforts. Next, we selected two critical systems from both the Clerk's and SAA's Y2K Plans and three projects from the CAO Y2K Program Plan based on project mission criticality, reported status, visibility, and other risk factors. We reviewed testing in detail because thorough testing is needed to ensure that work done in the prior phases has adequately prepared the House to meet the Y2K challenge.

Additionally, we performed a limited review of the CAO's progress in assisting Member and Committee offices to prepare for Y2K. In our consulting role, we attended BCCP committee meetings, provided support, research assistance and evaluations of best business practices to assist in the House's Y2K contingency planning efforts. Finally, we followed up on the status of prior audit recommendations.

Our current review covered the period January 1999 through December 1999.

Internal Controls

The internal controls over the House Y2K initiative were adequate.

Prior Audit Coverage

The OIG's involvement in the House's Y2K process started in December 1996, when we recommended that the CAO develop a comprehensive Y2K plan. Since then, we have provided both audit and consulting services to the House Officers. The OIG first addressed Y2K issues in an audit report entitled, *Improvements Are Needed In The Management And Operations Of The Office Of The Chief Administrative Officer*, (Report No. 96-CAO-15, Finding F), dated December 31, 1996. The finding concluded that House Y2K activities needed the benefit of a team leader assignment, an assessment of office level systems within the House environment, and an analysis to determine the impact of phasing out legacy application systems. The audit recommended that the CAO prepare a comprehensive Y2K strategy for the Committee on House Oversight's (CHO)[1] review and approval. The Acting CAO concurred with the audit recommendation. Subsequent management actions were adequate to close the recommendation.

The OIG conducted its first follow-up audit entitled, *House Needs to Refocus Its Efforts To Meet The Year 2000 Deadline*, (Report No. 97-CAO-13), dated September 29, 1997. This audit recommended that House Information Resources (HIR) institute project management controls over the process, revise and prepare follow-on documentation related to the Y2K plan, revise Y2K cost estimates, and update budget requests. Further recommendations were to coordinate data exchange issues with external organizations, adopt standard Y2K compliance contract language for information technology procurements, and expedite decisions regarding the replacement of mission critical information systems. The CAO concurred with the recommendations. Subsequent management actions were adequate to close the recommendations.

The OIG conducted its second follow-up audit entitled, *Prompt Actions Needed To Meet The Year 2000 Deadline* (Report No. 99-CAO-01), dated January 8, 1999. This audit was the third in a series of periodic reviews planned to monitor the House's progress in meeting the Y2K deadline. The overall audit objectives were to assess the House Y2K program as it related to current status, timetable for completion, and the allocation of priorities and resources. In addition, we evaluated the risk of disruption to essential House activities in Y2K. The audit methodology consisted of an overall review and assessment of the CAO's Y2K Program Plan and a detailed review of 15 individual Y2K projects based on mission criticality, reported status, visibility, and other risk factors.

The OIG conducted its third follow-up audit entitled, *Year 2000 Testing and Contingency Planning Efforts Should Minimize Risk of Date Related Failures* (Report No. 99-CAO-09), dated December 21, 1999. The audit objectives were to assess the status of the CAO unit, integration, acceptance and end-to-end Year 2000 compliance testing efforts; the adequacy of the Business Continuity and System Contingency Plans; and status of prior audit recommendations. The audit methodology involved selecting three projects from the CAO Year 2000 Program Plan for detailed review based on mission criticality, reported status, visibility, and other risk factors affecting the testing efforts. No recommendations were issued as a result of this review.

[1] The 106th Congress changed the name of the Committee on House Oversight (CHO) to the Committee on House Administration (CHA).

II. RESULTS OF REVIEW

Our review has determined that Member and Committee offices, the Clerk, SAA, and CAO have taken reasonable action to test and assure the Y2K compliance of their systems and prepare contingency plans as evidenced by the following summary of specific actions taken by each office. A detailed list of each Officer's projects/systems and Y2K compliance status is located in Exhibits 1-3.

Member and Committee Offices

HIR prepared a plan to assist Member and Committee offices to prepare for Y2K. The CAO also appointed a project manager and assigned personnel to work on this Y2K initiative. Specifically, HIR has provided the following services to all Member and Committee offices in support of the Y2K initiative:

- Prepared and distributed a "*Smart Guide*" to assist Member offices to understand and comply with Y2K requirements;
- Distributed "*Ymark2000*"--a software package which identifies firmware date problems on Member office hardware--and "*One Touch*" CD which contains Y2K software fixes;
- Held seminars at the Member office level to identify Y2K problems; and
- Staffed the Help Desk with system engineers to assist Member offices with Y2K fixes.

Based on discussions with the project leader, assigned personnel, and a review of the CAO's documentation supporting the progress of Member and Committee offices in preparing for Y2K, we concluded that the Member and Committee offices, in conjunction with HIR, had made reasonable efforts to correct Y2K problems associated with Member and Committee office-owned computer systems. As of December 17, 1999, HIR completed the assessment of these computer systems and identified 35 computers in the Member offices that are not Y2K compliant. However, these noncompliant computers are stand alone, and, as such, do not create a risk to the House.

HIR has provided Member district offices with the "*One Touch"* CD. To date, all reported Y2K problems in district offices that have used this CD have been resolved by using the Y2K Help Desk. Once Member DC offices have all been completed, HIR will make personnel available to assist any remaining district offices until they are Y2K compliant. HIR has also contacted system integrators in various district office locations to provide assistance.

Clerk

The Clerk prepared a Y2K Plan, appointed a project leader, and assigned personnel to work on the initiative. Based on discussions with the project leader and assigned personnel as well as reviews of testing plans (see Exhibit 1), we concluded that the Clerk made reasonable efforts to correct Y2K problems associated with FileNet and Electronic Voting System (EVS). In addition, tasks were prioritized for mission critical projects, and target dates were prepared. Finally, vendors were requested to certify appropriate products for Y2K compliance. Our review of the Clerk's testing of FileNet and EVS revealed the following internal control strengths,

which will minimize the risk of date related failures in House systems on or after January 1, 2000. Specifically, we noted that:

- Testing phases and dates covered the test scenarios recommended in the GAO's *Year 2000 Computing Crisis: A Testing Guide.*
- Hardware and operating systems were updated to Y2K compliant versions.
- Test reports showed documentary evidence supporting the execution of critical Test Plan steps.
- The Y2K Coordinator independently monitored testing of system changes made by the System Manager.
- Vendor websites are monitored for the latest Y2K information that could affect Clerk processing.

SAA

The SAA prepared a Y2K Plan, appointed a project leader, and assigned personnel to work on the initiative. Based on discussions with the project leader and assigned personnel as well as reviews of testing plans (see Exhibit 2), we concluded that the SAA made reasonable efforts to correct Y2K problems associated with the Parking Office Permit System and House ID Badging system. In addition, tasks were prioritized for mission critical projects, and target dates were prepared. Finally, vendors were requested to certify appropriate products for Y2K compliance. Our review of HIR and SAA Y2K testing of various system components revealed the following internal control strengths, which will minimize the risk of date related failures in House systems on or after January 1, 2000. Specifically, we noted that:

- The Test Plan phases and dates covered test scenarios recommended in the GAO's *Year 2000 Computing Crisis: A Testing Guide.*
- Test reports showed documentary evidence supporting the execution of critical Test Plan steps.
- Failed Test Plan results were documented and supported in the Deviation Reports.
- Deviations in the Test Plan results were resolved in an appropriate manner.
- Both functional and Y2K compliance testing were performed.
- The SAA System Administrator signed the Test Plan and report.
- The SAA provided written acceptance of system compliance.

CAO

The CAO prepared a Y2K Plan, appointed a project leader, and assigned personnel to work on the initiative. Based on the projects reviewed (see Exhibit 3), we concluded that the CAO Y2K compliance testing methodology was both structured and adhered to best business practices. For the systems reviewed, the Test Teams complied with the Y2K Test Plan procedures. Also, the CAO's House-wide BCCP, while not finalized as of the end of our fieldwork, complied with best business practices and adequately addressed threats that may affect House operations as a result of potential Y2K problems. The House is preparing its BCCP in concert with the Legislative

Branch Y2K Coordination Group Capitol Complex contingency planning. This effort had not been finalized[2] at the end of fieldwork.

Our review of CAO testing processes revealed the following internal control strengths that will minimize the risk of date related failures in House systems on or after January 1, 2000. Specifically, we noted that:

- The Y2K Test Plan phases and dates covered the test scenarios recommended in the GAO's *Year 2000 Computing Crisis: A Testing Guide*.
- Test Reports providing documentary evidence supporting the execution of critical Test Plan steps were required.
- Automated testing tools were available and used effectively and efficiently.
- Deviations in testing results were required to be captured, logged and tracked through successful resolution.
- Separation of duties between the Application Specialists, Test Team, and system users was defined to help ensure integrity of the testing process.
- Users were required to provide written acceptance of system compliance based upon their independent functional, performance, and security testing.
- Test monitoring was performed and documented through Test Team status reports and the quarterly Y2K Program Plan.

Conclusion

Based on our review, it is our opinion that the House reasonably followed best business practices and GAO guidance in testing critical information technology computer systems and developing contingency plans. This approach should minimize the risk of date related failures on or after January 1, 2000. The OIG will continue to assist House Officers with solutions to Y2K issues.

[2] In early 1999, the Architect of the Capitol organized and began coordinating the efforts of the Legislative Branch Year 2000 Coordination Group. The group consists of representatives from every Capitol Complex agency, including the United States Capitol Police, and several agencies outside the Capitol Complex, including the General Accounting Office and Government Printing Office. The group is preparing a Day 1 Guide that addresses a contingency strategy for identifying and mitigating Year 2000 impacts on the Capitol Complex. A key component of the Guide is the Critical Incident Command Center (CICC) housing a team of decision makers and emergency response personnel during the New Year's weekend.

Exhibit 1

Office of the Clerk Y2K Compliance

System	Status	Comments
1. AREV (Front Office) Personnel System	Y2K compliant.	HIR certification received.
2. AREV (Page School) Page School Scheduling	Y2K compliant.	Replaced with Y2K COTS product (Administrator Plus from Rediker & Gradequick by Jackson)
3. Clerk's Web Site all HTML display files	Y2K compliant.	All software is Y2K compliant. Y2K contingency plan was reviewed by OPS 10/25/99.
4. Docucolor 40 OPS Cannon Building.	Y2K compliant.	Received certification documents from Xerox.
5. Docutech Systems 6135 LRC Cannon Building	Y2K compliant.	Received certification documents from Xerox.
6. Docutech Systems 6180 Ford Building	Y2K compliant.	Received certification documents from Xerox.
7. Electronic Voting System	Y2K compliant.	Custom code placed in production 1/27/98. Documentation of testing process/results reviewed and approved by IG (October 1999). Additional testing conducted in August and September 1999.
8. FEC-Campaign Reports Clerk Federal Election Report	Y2K compliant	FEC informed Clerk they are fully compliant.
9. FileNet System Lobby Disclosure	Y2K compliant.	Placed in production 8/6/1999. Documentation of testing process/results reviewed and approved by IG (October 1999)
10. FileNet System Workstations	Y2K compliant.	N/A
11. FileNet System Federal Election Reports Mainframe: (Adabas/Natural)	To retire 12/31/1999.	This portion of the system will be retired as the records are available at the FEC.
12. FileNet System Federal Election Reports Clerk/FileNet/UNIX/PC	To retire 12/31/1999.	This portion of the system will be retired as the records are available at the FEC.
13. FileNet System Financial Disclosure	Y2K compliant.	Placed in production 7/20/1998. Documentation of testing process/results reviewed and approved by IG (October 1999).
14. FileNet System Server Software	Y2K compliant.	Upgraded AIX and imaging software.
15. FMS Financial Disclosure GS-16 Reports	Y2K compliant.	The current FMS system is being replaced and this in included in the replacement Y2K compliant system.
16. GPO Congressional Record, Journal and Bills	Y2K compliant.	Completion date is the receipt date of GPO's Y2K BCCP. GPO reports their software is fully compliant.
17. House Floor Audio System	Y2K compliant.	Portable system was set up and tested 11/8/1999.
18. House Publications System Committee Hearings	Y2K compliant.	Completion date is the receipt date of GPO's Y2K BCCP. GPO reports their software is fully

Exhibit 1

Office of the Clerk Y2K Compliance

System	Status	Comments
		compliant.
19. LIMS Bill Status and Calendar Production	Y2K compliant.	Placed in production 1/4/1999. Additional testing with Y2K dates completed April 1999. No problems found.
20. Members' Badging System	Y2K compliant.	N/A
21. Official Reporters CaseCatalyst	Y2K compliant.	Novell server being taken down—users internal office files 90% on NT Network now. Completion pending install of recently acquired PC equipment upgrades for Official Reporters Offices. Migration from Novell based Premier Power product to Windows NT CaseCatalyst product is completed.
22. Official Reporters Hearing Transcript Accounting System	Y2K compliant.	Replacement system developed by Clerk staff.
23. Publications Services Elections	Y2K compliant.	N/A
24. Publications Services Binding	Y2K compliant.	N/A
25. Publications Services Pink Reqs	Y2K compliant.	N/A
26. Publications Services White Reqs	Y2K compliant.	N/A
27. Publications Services Telephone Book	Y2K compliant.	N/A
28. Publications Services Ad Hoc Publications	Y2K compliant.	N/A
29. System Infrastructure	Y2K compliant.	Clerk's Lans and PCs were upgraded to current technology during the 104th Congress.
30. UPS EVS/House Floor/Network servers	Y2K compliant.	Received manufacturer's documentation for Y2K compliance for best UPS (EVS) and Equinox terminal servers under House Floor.
31. Xerox/Fax Machines	Y2K compliant.	Received certification documents from Xerox.

Exhibit 2

Office of the Sergeant at Arms Y2K Compliance

System	Status	Comments
1. Parking Office Permit System (POPS)	Y2K compliant.	Tested using CAO plan.
2. House ID Badging System	Y2K compliant.	Tested using Senate plan.

Exhibit 3

Office of the Chief Administrative Officer Y2K Compliance

Projects	Status	Comments
1. CAO Computers-Member Office and Committee Outreach	Y2K compliant.	Statistics have been collected on over 11,000 computers in the House, representing all Washington Offices and most District offices. Of these 11,000 computers, there are currently 38 PC's that fail the YMARK2000 test of the real-time clock and the BIOS (data as of September 30, 1999). CAO staff is working with those offices to replace the PCs as soon as possible.
2. Communications Hardware and Software	Y2K compliant.	All products installed by House staff have been upgraded to their Y2K-compliant versions. There is one item tracked in the Communications project, internet service from Cable and Wireless, that has not been certified compliant by the vendor. That work is scheduled for completion by Cable and Wireless during the 4th quarter of 1999.
3. FFS Core System Upgrade for Y2K	Y2K compliant.	FFS was upgraded to a Y2K compliant version in September 1998.
4. FFS Custom Modules (AMS)	Y2K compliant.	Necessary upgrades have been made to the custom designed modules of the financial system that were performed by AMS.
5. FFS Custom Modules (ATS)	Y2K compliant.	Necessary upgrades have been made to the custom designed modules of the financial system that were performed by ATS.
6. Fixed Asset Replacement, and 7. Fixed Asset Contingency	Y2K contingency project compliant.	The replacement system, FAIMS, was not completed. The contingency, renovation of four legacy systems, was completed in September 1999 and is in production.
8. Legislative Information Management System (LIMS)	Y2K compliant.	Remediated to Y2K compliance.
9. Member Office and Committee Accounting	Y2K compliant.	The Y2K-compliant version of Office Accounting for Windows (OAW) has been installed. However, because Microsoft has announced that they will terminate support for the version of FoxPro used by OAW at the end of 1999, OAW is being converted to run under Visual FoxPro6.0. While this is not, strictly speaking, a Y2K issue, this is a convenient time, because of the planned one-touch effort in offices, to install the technology upgrade. In addition MYOB, a commercial, off-the shelf, package that has been tailored for House use, is available for Committees and Members who may prefer this as an alternative. Finally, provision of a personnel

Exhibit 3

Office of the Chief Administrative Officer Y2K Compliance

Projects	Status	Comments
		module in OAW has been approved. Because this effort is likely to extend into 2000, a contingency for Member Clerk-Hire has been developed to permit continued use of that application after December 31, 1999.
10. Messaging Servers	Y2K compliant.	All servers and all operating systems software are now compliant. Advanced date testing was performed to validate vendor certifications. All systems passed.
11. Staff Payroll Replacement, and 12. Staff Payroll Contingency	Y2K contingency project compliant.	Request for proposals for a replacement system has been approved and released by the Committee on House Administration. Solicitation, selection and implementation of the new system are expected to take two years. As a contingency, September staff payroll utilized the renovated, Y2K compliant version of the staff payroll system.
13. Member Payroll Replacement, and 14. Member Payroll Contingency	Y2K contingency project compliant.	Member payroll was completed in September 1999 and the payroll for October 1 was generated from the new Member Payroll system. A Member payroll contingency was completed in July 1999, but not needed.
15. AD HOC Applications	Y2K compliant.	These applications were designed in HIR and run on platforms other than the mainframe, supporting Members, Committees, or other offices of the House. All are either compliant or scheduled for retirement before 2000.
16. Consolidated Common Gateway Interface (CGI)	Y2K compliant.	Web based applications have been assessed and renovated as necessary.
17. Food Services Auditing Tool	Y2K compliant.	Replaced desktop program to receive register data and provide independent audit capability of vendor receipt calculations.
18. Mainframe Applications	Y2K compliant.	Nine applications will be retired before January 2000. Work on the remainder has been completed.
19. Mainframe CICS and Software AG Products	Y2K compliant.	Necessary upgrades have been made.
20. Mainframe Languages and Compilers, and 21. Mainframe Operating Systems	Y2K compliant.	On January 3, 1999, the HIR mainframe was successfully converted to OS 390 as the production operating system. OS 390 is the Y2K-compliant operating system for the enterprise server. In addition, the operating system support products are continuing their conversion with 4 products remaining to be converted. Finally, the operating system and

Exhibit 3

Office of the Chief Administrative Officer Y2K Compliance

Projects	Status	Comments
		support products are being tested with future dates on the RISC 6000 test bed that was recently installed. While the House has vendor statements of compliance for all products, the testing with the system date advanced past December 31, 1999, provides additional assurance that the products will function properly.
22. ISIS-Administrative 23. ISIS-Informational 24. MIN-ISIS-LRS-Legislative 25. MIN-Bulletin Boards 26. MIN-Informational 27. MIN-ISIS Newswires 28. MIN-Administrative 29. MIN-ISIS Federal Funding	Y2K compliant.	All MIN services were migrated from the mainframe to other sites or retired as of June 1999. LRS and ISIS services were migrated or retired as of December 1998.
30. Non Computer Office Equipment	Y2K compliant.	Vendors of all other CAO-supplied office equipment have been contacted and vendor information on those products has been summarized in the information packet provided to Members, Committees and other offices.
31. OSS Point of Sale System, and 32. OSS Point of Sale Contingency	Y2K contingency project compliant.	Cafeterias and the Office Supply Store systems have been assessed. A vendor has replaced the register system in all House cafeterias, except Ford, which was upgraded by the CAO (Food Services). The necessary replacement of the office supply store register system is underway; however, delays in the project have led to the development and implementation into production of a contingency system effective November 1999.
33. Procurement Desktop-Fixed Asset Purchasing	Y2K compliant.	Replaced vouchering functions of the existing Office Systems Management system.
34. Security (HIDACS) System	Y2K compliant.	Upgraded the security system for the HIR computer room and other offices.
35. Web Server hardware and Software	Y2K compliant.	All servers and operating systems software are now compliant. Advanced date testing was performed to validate vendor certifications. All systems passed.