



**REPORT ON CONTROLS
PLACED IN OPERATION AND
TESTS OF OPERATING EFFECTIVENESS
FOR CUSTOM DATA PROCESSING, INC.**

**For the Period July 1, 2001
through June 30, 2002**

**EDWARD B. HATCHETT, JR.
AUDITOR OF PUBLIC ACCOUNTS
WWW.KYAUDITOR.NET**

**144 CAPITOL ANNEX
FRANKFORT, KY 40601
TELE. (502) 564-5841
FAX (502) 564-2912**



Edward B. Hatchett, Jr.
Auditor of Public Accounts

To the People of Kentucky

Honorable Paul E. Patton, Governor

Marcia R. Morgan, Secretary, Cabinet for Health Services

Jack H. Marston, President, Custom Data Processing, Inc.

The enclosed report prepared by Crowe, Chizek and Company LLP, Certified Public Accountants, presents the report on controls placed in operation and tests of operating effectiveness for Custom Data Processing, Inc. for the period July 1, 2001 through June 30, 2002. Custom Data Processing, Inc. is a service organization for the Cabinet for Health Services.

We engaged Crowe, Chizek and Company LLP to perform the SAS 70 audit of Custom Data Processing, Inc. We worked closely with the firm throughout the audit and report review process.

Respectfully submitted,

Edward B. Hatchett, Jr.
Auditor of Public Accounts

Enclosure

Commonwealth of Kentucky

Cabinet for Health Services



Custom Data Processing, Inc.

**REPORT ON CONTROLS PLACED IN
OPERATION AND TESTS OF
OPERATING EFFECTIVENESS**

**For the Period July 1, 2001
Through June 30, 2002**

Prepared by:



CROWE CHIZEK

**Crowe, Chizek and Company LLP
Information Risk Management Practice
330 East Jefferson Boulevard
South Bend, IN 46624
<http://www.crowechizek.com>**

**Commonwealth of Kentucky
Cabinet for Health Services**



Custom Data Processing, Inc.

**REPORT ON CONTROLS
PLACED IN OPERATION AND
TESTS OF OPERATING EFFECTIVENESS**

**For the period July 1, 2001
Through June 30, 2002**

Table of Contents

REPORT OF INDEPENDENT ACCOUNTANTS	1
DESCRIPTION OF POLICIES AND PROCEDURES PLACED IN OPERATION Provided By Custom Data Processing	
OVERVIEW	3
GENERAL CONTROLS	4
Organization and Administration.....	4
Disaster and Contingency Planning.....	5
Software Implementation, Maintenance, and Documentation.....	8
Computer Operations.....	10
Physical Security.....	14
On-line Security.....	15
APPENDICES	
Appendix A -- Test of Operating Effectiveness.....	19
Appendix B -- User Control Considerations.....	31
Appendix C -- Organizational Chart.....	33



REPORT OF INDEPENDENT ACCOUNTANTS

Commonwealth of Kentucky
Cabinet for Health Services
Frankfort, Kentucky
and
Custom Data Processing, Inc.
La Grange, Illinois

We have examined the accompanying description of controls related to the Commonwealth of Kentucky Cabinet for Health Services (CHS) system applications specifically consisting of Patient Encounter (to include the Contract Code Charge Module), Women Infant & Children (WIC), Home Health, Payroll, Accounts Payable & Financial Reporting System (AP&FRS), Fixed Assets, and Bank Reconciliation applications running on Windows NT servers of Custom Data Processing, Inc. (CDP). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of CDP's controls that may be relevant to CHS' internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and CHS applied the controls contemplated in the design of CDP's controls, and (3) such controls had been placed in operation as of June 30, 2002. The control objectives were specified by the Auditor of Public Accounts (APA) and considered by both CHS and CDP. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

As discussed in the accompanying description, CDP has not designed procedures to formally assess the risk levels for preventing unauthorized or undetected access to CDP's information resources. These deficiencies result in the controls not being suitably designed to achieve Control Objective 5: "Controls provide reasonable assurance that logical access to programs and data is limited to properly authorized individuals."

In our opinion, the accompanying description presents fairly, in all material respects, the relevant aspects of CDP's controls that had been placed in operation as of June 30, 2002. Also, in our opinion, except for the matters described in the preceding paragraph, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the internal controls contemplated in the design of CDP's controls relating to the systems at CDP.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Appendix A, to obtain evidence about their effectiveness in meeting the control objectives, described in Appendix A, during the period from July 1, 2001 to June 30, 2002. The specific controls and the nature, timing, extent, and results of the tests are listed in Appendix A. This information has been provided to user organizations of CDP and to their

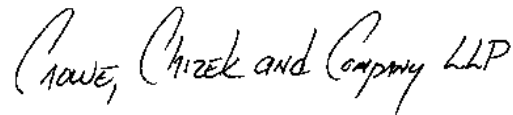
auditors to be taken into consideration, along with information about the internal control at CDP, when making assessments of control risk for user organizations.

In our opinion the controls that were tested, as described in Appendix A, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Appendix A were achieved during the period from July 1, 2001 to June 30, 2002. However, the scope of our engagement did not include tests to determine whether control objectives not listed in Appendix A were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Appendix A.

The relative effectiveness and significance of specific controls at CDP and their effect on assessments of control risk at CHS and its agencies are dependent on their interaction with the controls and other factors present at CHS and its agencies. We have performed no procedures to evaluate the effectiveness of controls at CHS or its agencies.

The description of controls at CDP is as of June 30, 2002 and information about tests of the operating effectiveness of specified controls covers the period from July 1, 2001 to June 30, 2002. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls at the CDP is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions."

This report is intended solely for use by the management of Client, its customers, qualified prospects and the independent auditors of its customers."



Crowe, Chizek and Company LLP

South Bend, Indiana
July 3, 2002

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

OVERVIEW

Custom Data Processing, Inc. (CDP) has operated as a systems integrator for various clients since its inception in 1964, and has served the Commonwealth of Kentucky Cabinet for Health Services (CHS) in this capacity since 1981. The services provided include the supply and maintenance of functional and financial software applications, the processing of data, technical support and training, and the provision of data telecommunications. Of the software applications provided, seven are financial audit-significant to CHS. These systems include: Patient Encounter (to include the Contract Code Charge Module), Women Infant & Children (WIC), Home Health, Payroll, Accounts Payable & Financial Reporting System (AP&FRS), Fixed Assets, and Bank Reconciliation applications.

The centralized processing center within CDP's organization is located in La Grange, Illinois. All financial audit-significant systems are running on a Windows NT platform, processed on a Compaq Proliant 6400 series server. The job scheduling software and other ancillary applications were converted from the Unisys mainframe to Windows NT systems during the report timeframe. Computer operations and network support personnel reside at the La Grange location. The Compaq Proliant 6400 series server housing the Fixed Asset, Home Health Care, Payroll, Accounts Payable, Financial Reporting and Bank Reconciliation Systems, also resides at the La Grange location. A redundant hot site, owned and operated by CDP, is located at CDP's Frankfort, Kentucky facility where software developers, user support, and technical personnel also reside. Support offices serving other customers also exist in Tucson, Arizona and Salt Lake City, Utah.

Since the early 1980's, CDP has focused its systems integration and outsourcing efforts on the healthcare and environmental health industries. Within the Commonwealth of Kentucky, CDP has built the largest Local Health Network in the country. Twenty-two on-line/real-time applications are operational on this network via CDP's Service Center. The Local Health Network (LHN) is composed of approximately 267 physical sites with approximately 3,000 attached devices. These devices consist of primarily state purchased personal computers and printers.

The communication links with both the State and local agencies in Kentucky are utilizing industry standard TCP/IP protocols. In very limited instances CDP is still using the Unisys Poll/Select protocol to facilitate communications between CDP and State agencies. This is primarily used as a back-up facility for CHS. The communications network is primarily under control of the Governor's Office of Technology (GOT). The State has a network in place commonly referred to as The Kentucky Information Highway (KIH) and is used by almost all of the health departments in the state to communicate with CDP.

Significant Events in the Past Twelve Months

The most significant events during the past twelve months were:

- The introduction of new WIC reports.
- The new Environmental System Lab functionality.
- General improvements to the Home Health Care System.
- The first usage of Visual Basic front-end screens.

Identification of Control Objectives and Tests of Operating Effectiveness related to the descriptions provided within this section are listed in Appendix A.

User Control Considerations, which complement the controls in place for CDP, are listed in Appendix B.

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

GENERAL CONTROLS

General Controls are those policies, procedures, and safeguards that relate to all internal information system activities. Their purpose is to ensure the continued, consistent, and proper functioning of information systems by controlling, protecting, and maintaining application software and computer operations. The controls are divided into the following six areas:

- Organization and administration,
- Disaster and contingency planning,
- Software implementation, maintenance, and documentation
- Computer operations,
- Physical security, and
- On-line security.

It should be noted that, if these areas are not segregated, they can overlap to affect all information system activities. As a result, the adequacy of these controls is considered fundamental to the effectiveness of specific applications and weaknesses within these General Controls can have pervasive effects that are detrimental to many applications.

Organization and Administration

CDP is organized geographically with functional work groups located in different offices, which provides adequate separation of duties. The functional groups are: Programming, Networking, and Customer Support. A manager, who reports directly to the Vice President, directs each group; the Vice President reports to the President. See the accompanying organizational chart in Appendix C.

CDP maintains an insurance package that includes IS equipment, media, extra expense, errors and omissions, general liability, building and contents casualty coverage, workmen's compensation, umbrella liability coverage, professional liability, and employee dishonesty coverage.

Control Environment

CDP's operations are under the direction of the Vice President, General Managers, and functional level managers. Collectively, management is responsible for ensuring control in the production area (which includes Operations and Customer Support), Application Development, and Telecommunications Networking.

The composition, activities, and attitudes of management attempt to ensure that employees maintain integrity and are knowledgeable of their responsibilities in CDP's operations. Numerous human resource policies have been developed to contribute to CDP's overall control environment. These policies relate to work hours, employment benefits, vacations, and general security. Furthermore, in order to help ensure employee competence, all candidates for employment are required to have references. These references are checked prior to formal employment. Police background checks are also performed on all new employees.

Management attempts to ensure the segregation of duties as a control activity. Management also attempts to ensure organizational independence. CDP is organizationally independent of customers, as all

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

customers are external to the CDP organization. In the course of their normal duties, CDP personnel do not authorize or initiate transactions nor are they involved in the correction of transactions with errors.

Risk Assessment

Risk assessment is a continual process conducted by CDP management. Management sets clear objectives and initiates steps to identify key risks affecting the company and its objectives. These steps are based on reliable and timely information obtained from knowledgeable sources.

Communication

Management has established an organizational structure and set a tone that facilitates the communication of important business information. Management meetings are conducted frequently at both the senior and middle management levels. Further, CDP employees are encouraged to share information they possess that might affect business operations.

Monitoring

Management attempts to ensure that an appropriate level of monitoring is conducted throughout the course of CDP operations. This monitoring is performed over a wide variety of functions at all levels of the organization.

Disaster and Contingency Planning

CDP has various controls in place to mitigate the potentially disruptive effects or damage caused by fire, water, electrical storms, vandalism, and other factors.

Frankfort, Kentucky

Technical support, communications, and application software and documentation maintenance are the primary functions occurring at the Frankfort facility. Frankfort also has secondary roles as an off-site tape storage facility and a business recovery hot site for the La Grange, Illinois Operations Center.

The backup computers, Compaq servers, front-end processor, and operations terminals are located in a self-contained communications and hardware area within the facility. This backup hardware is stored on a raised floor in a climate-controlled room. All of the server equipment is also protected by uninterruptible power supplies and surge protection devices.

La Grange, Illinois

Systems programming (selection, implementation, and maintenance), system security, network monitoring, scheduling, computer operations, and data archival/storage are the primary responsibilities of the La Grange, Illinois facility.

To prevent or mitigate the operationally disruptive effects of a fire before it becomes severe, a heat detection and alarm system has been installed throughout all areas of the facility, including the computer operations room. In addition to triggering a sprinkler system, the system will electronically notify a private security company who will contact the fire department and appropriate CDP personnel.

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

A fireproof tape and media vault used for on-site storage of back-up tapes and sensitive documentation is located within the computer operations room. The vault is sturdily constructed to resist impact damage as well.

To ensure the computer and printing equipment is maintained at the correct temperature and humidity level, a self-monitoring air conditioning/control system is installed specifically for the computer operations room. In case of failure in the primary air conditioning unit, a back-up unit designed to provide temporary cooling capability until the primary unit can be repaired or replaced is kept within the computer operations room.

An uninterruptible power supply (UPS) unit, housed within the computer operations room, automatically supplies conditioned power in the event of an interruption of utility power. The UPS can supply approximately 30 minutes of power that will facilitate an orderly, staged shutdown of devices should the power outage last beyond ten minutes. Shutdown procedures have been developed and documented and are available to operations personnel. The battery level and voltage of the UPS is checked weekly by CDP personnel. Further, should a power outage last longer than 30 minutes, CDP has also installed a generator that can be manually activated. The generator is gas-powered and will continue running as long as there is gas in the generator tank. The generator is also checked periodically by the Operations Manager to ensure that it is working properly. The Operations Manager keeps a log of all UPS and generator tests.

To ensure that lost or corrupted files can be restored, full system backups (data files, system software, and applications) are made daily Monday through Friday and rotated to an off-site storage facility on a three-day cycle (the previous two sets of tapes are stored off site while the third most recent set is kept in a locked case within the media vault in the CDP computer operations room). CDP has an on-going contract with a third party vendor for off-site storage of the backup tapes. The vendor will pick up the current tapes and return the oldest tape to CDP every morning. CDP personnel sign and retain a copy of the receipt that indicates the date and the number of tapes sent off site. CDP tapes are stored in a temperature and humidity controlled vault at the vendor's location. Although backups are rotated off-site on a three-day cycle, more than three days worth of backups are available on-site. Tape backups are kept for varying intervals. For example, the retention cycle for the systems resource pack is one month, while the retention cycle for the backup of executable code is five days. Currently a duplicate copy of archived data from the PES, Patient Purge, History Purge, and Appointment Purge is sent to Frankfort. The PES purges are processed every other month.

Business Resumption

CDP has developed a Business Resumption Plan to ensure that, in the event that the CDP La Grange computer center is rendered inoperable, operations can be smoothly transitioned to the CDP Frankfort disaster recovery site within a 48-hour time frame.

CDP Frankfort has three Compaq 1600 series servers, one Compaq 6400R, one Compaq Proliant 5500 series server, and various other servers on site with disk configurations that mirror those of CDP La Grange. Identical communications processors (USA FEP) are present at both sites. All operating system and utility software source media and documentation reside at both locations.

Data and application files, as well as communication configurations, are backed up each night on 4mm DAT tape media. These tapes are then taken to an off-site location that will always house the two most recent generations of backup tapes. All files of archived data are created on 4mm DAT tape media. A

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

copy of these tapes is made at the time of creation and sent to the Frankfort site. The Frankfort site will always have the current tapes of any historical information needed for application processing.

The CDP La Grange staff has been divided into two teams. Several "North Transition Team" members will be the first to arrive in Frankfort and will be responsible for loading out application and data files, bring up the system, and establishing the "on-line" environment. Remaining members of the "North Transition Team" will leave Chicago within 24 hours of the departure of the initial group and will handle the scheduling, operations, and general customer support, once CDP South is operational. The CDP La Grange "Home Team" will stay in the Chicago area and initially be responsible for making airline, rental car and hotel reservations for the "North Transition Team" members. All other CDP North personnel will remain on standby status.

CDP Frankfort will have a "Transition Team" responsible for the initial preparation of the Frankfort site and the FlexServe communications switch from La Grange to Frankfort. All other CDP South personnel will be notified of the situation. Once the CDP South site becomes operational and CDP "North Transition Team" members have arrived at CDP South, Kentucky State personnel and hub sites will be notified via the Main Kentucky Users bulletin board that CDP North is temporarily down, that CDP South is operational, and that all customer support needs should be directed to a specified phone number at CDP South.

A checklist of chronologically ordered procedures to be performed in the event of a disaster is included in the CDP Business Resumption Plan notebook. Additionally, detailed instructions relating to each procedure, vendor contact information, CDP personnel information, priority schedules, and hub site information are included in cross-referenced appendices within the same notebook.

The CDP Business Resumption Plan is tested at a minimum of every twelve months. The last test was performed successfully in March 2002. CHS personnel perform the connectivity testing to ensure adequate recovery of the system. The CHS Contract Administrator signs-off indicating the test was performed according the contract specifications. CDP retains the system logs of the test for a twelve-month period.

A redundant T-1 data connection has been installed between GOT and the La Grange facility. A router has been placed at GOT which would be activated if a disaster were to occur at the Frankfort facility. This redundant connection will be tested as part of the disaster recovery test.

In the normal course of daily operations, the CDP Frankfort office is viewed as a typical hub site. In the event of a disaster at the Frankfort facility:

- A. Necessary programming and support staff would be relocated to the La Grange office.
- B. Customer support, emergency fixes and software changes would be handled by La Grange personnel until Frankfort staff is situated.
- C. Kentucky State personnel and hub sites would be notified via the main Kentucky users bulletin board.

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

Software Implementation, Maintenance, and Documentation

The change management process for all applications begins when CDP receives a System Change Request Form (SCRF) from the CHS. The form includes a brief description of the change being requested and the contact information for the requesting individual. The form must also include authorizing signatures from CHS. Specifically, the CHS contract administrator and the CHS department manager (for the department requesting the change) must sign the form. The Louisville Health Department, Lexington Health Department, Bowling Green Health Departments, Northern Kentucky Health Departments and other non-state-wide locations are exceptions to the change request process. There are key people located in each of these locations by whom an informal request for changes can be made to the CDP general manager or programming manager. Because these requests can be generated via CDM message, fax or through electronic mail, a program project sheet will be the primary piece of documentation associated to the project.

Once CDP receives the completed SCRF, the CDP General Manager (or a Programming Manager) reviews the request, composes a cost estimate (a separate section of the same form), and records the details of the request in the CDP project tracking system with a CDP project number. The overall estimate entails both time and cost (to CHS) estimates. The estimating manager also ascertains the degree to which the proposed change would affect current processing. This factor could affect the scope of the estimate. Once the cost estimate has been completed, the CDP General Manager or Programming Manager will sign the cost estimate and return the form to CHS.

After the preparation of the CDP cost estimate, CHS reviews the estimate and determines whether to proceed. If CHS decides to proceed, the CHS Contract Administrator and the CHS Department Manager will sign the form to denote final authorization of the change to be performed. The form is then returned to CDP.

The General Manager or a Programming Manager assigns the change to a programmer upon receipt of the fully authorized SCRF. The assigned programmer is responsible for performing the change and testing it on the test system. The assigned programmer also prepares any supplementary user documentation. In addition, the programmer will make a note as to (1) what changes were made, (2) when, and (3) which programmer made the change in the program header. However, documentation in the header is not required. Upon completion and successful testing of the change, the programmer submits a project sheet (printed from the on-line tracking system), that summarizes the work performed to the General Manager or a Programming Manager for review. If the project was a result of a perceived program error and not a user request, the programmer attaches to the project sheet a printout of the changes made to the program. Generally, the Programming Manager or General Manager reviews the changes informally. The reviewing manager will then confirm that the desired change has been performed. In the event that there is a major change requested, the General Manager or Programming Manager will thoroughly test the changes. Following this review, the General Manager signs the SCRF, and the form is returned to CHS for payment authorization.

Throughout the change process, the assigned programmer updates the on-line project tracking system. The tracking system reflects how much work (on an hourly basis) the programmer has invested in a project. The General Manager and Programming Managers review the tracking system weekly to ascertain overall development progress. This also helps management track open items. The Programming Manager prints a "Changes and Open Items" listing for senior management review bi-monthly so that senior management knows and understands what is happening at every level.

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

On the NT Server, the movement of code for modifications is controlled by a "loader" program. This program was implemented in March 1999 and is the only means of transferring source code into the programmers' development workspace for change purposes. Once the programmer "loads" the program into his/her workspace, the name of the program is changed in the directory, by adding the programmer's initials. If a programmer tries to load a program already checked out, they receive an error message stating that the program is currently being used by another programmer.

By requiring all staff members to use the "loader" program, CDP is provided with an audit trail of all source transfers. Additional security on the source code folders at the local area network (LAN) level has been put in place that prohibit workstations from using Windows Explorer "Drag and Drop" or DOS copies. The audit log of the "loader" program provides: 1) station, site number and programmer's initials; 2) a copy of the exact syntax entered by the staff member; 3) originating directory and source destination; 4) a date and time stamp along with the file size in bytes; 5) automatic archiving of original source code; and 6) audit logs showing the history of all "load/unload" activities.

Following the reviewing manager's approval, the programmer will compile the change and then submit a Program Implementation Request form for movement of the change into the live environment. On this form, the programmer indicates the name of the program to be implemented. The programmer also indicates the compile date and time. The form is sent to the Operations Scheduler in La Grange who adds the movement to the Operations schedule for the evening. All original source code is backed up daily prior to implementing any program changes and has a minimum retention period of two weeks.

The Operations staff in La Grange performing the move to production, upon completion of the implementation, verifies the compile date and time and matches the information provided on the Program Implementation Request. The following day, the Operations Manager reviews the daily processing log to ensure that all program modifications have a corresponding Program Implementation Request. If a change is noticed that is not supported by a Program Implementation Request, the Operations Manager will contact the programmer in charge of that particular application and require a form to be completed. The implementation program displays the system compile date and time for the changed program to ensure that it matches the compile date and time indicated on the Program Implementation Request.

Implementation of changes is coordinated between CHS and CDP. Meetings are periodically held (upon request or as often as monthly) to ascertain development progress and to clear rejected requests. Formal CDP Project Status meetings are held every week in La Grange, usually on Monday. These meetings are used to discuss the status of all on-going projects and any problems encountered. The General Manager and all Programming Managers are involved in these meetings. At the Frankfort location, the Programming Manager reviews a list of open requests on a weekly basis to determine which requests should take priority.

In certain situations where "emergency fixes" are requested and no SCRF is used, CDP initiates a project into its on-line Tracking System wherein a project control document is generated. This control document reflects the changes made and time accumulated. At completion time, the Programming Manager (or General Manager) reviews the project changes with the programmer and authorizes implementation. In these rare situations, the programmer will move the change into the production environment. However, they are also responsible for submitting a Program Implementation Request form. The implementation program will display the system compile date and time for the changed program to ensure that it matches the compile date and time indicated on the Program Implementation Request. The Operations Manager, who reviews the implementation request forms, assures that no unauthorized program changes have been implemented.

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

CDP uses only vendor supplied system software. Vendor supplied updates to the routing software are authorized, performed, tested, and loaded into production by the Systems Manager.

Since system software changes are at the discretion of the vendor, CDP merely follows the vendor's implementation instructions. No system software source code is available to CDP.

Any changes to the application source code are reviewed by the Programming Manager prior to implementation. Once approved, the programmers are required to complete a Program Implementation Form. These forms are then submitted to Scheduling for processing by the Operations staff during off-line hours. In the event that a program requires immediate implementation during on-line hours, the form is submitted to the Operations Manager or his designee for implementation (after approval). Additionally, implementation of any software changes are automatically listed on the Daily System Log (SPO Log). The SPO Log is a complete list of all events for the day. From this SPO Log file an extract of all software implementations is generated, printed, and will be attested to by the Operations Staff. Escalation procedures have been established in the event a program implementation is listed in the log and does not have a properly approved Program Implementation Form on file. Escalation events include discussing the change with the programming manager to restoring the application system and reprocessing the nightly update. This log is reviewed daily by the Operations Manager.

All vendors provide documentation updates with releases and fixes. Users are provided with any new documentation related to installation of fixes or new releases where their functions or interface are affected.

CDP has maintenance agreements with vendors for all system software and either receive notification or the actual tape when a vendor is ready to release separate program fixes or a new release. The CDP Systems Manager is responsible for evaluating the need to install new system software or upgrades to existing system software. He does so informally through discussions with the CDP President, network administrators, and programmers.

No vendor will exclusively modify CDP's copy of the systems software. This ensures that CDP system software can be upgraded without requiring additional planning or testing for CDP-specific customizations. All new or upgraded system software is tested in a separate test environment to ensure compatibility with other system software and with the current applications used by CHS. CDP personnel test the systems software until CDP is reasonably assured that no problems exist. Prior to implementation of fixes or new releases into the production environment, a complete system backup is performed. Should errors occur during changeover or if unforeseen processing problems arise after changeover, the previous version can be restored from the backup by reinitializing the processor and reinstalling the prior release.

Computer Operations

The vast majority of processing at CDP is recurring (i.e. running on the same days every month) rather than occurring randomly as needed. To assist operators in running the appropriate batch process and report jobs for any given day, CDP has developed a scheduling application (Operations Setup and Scheduling System) in-house. The system produces run sheets that list in their appropriate sequence all of the jobs that the Operator should ensure are run on the current day. The Operator uses the run sheets to determine which job should be started and any parameters which should be manually specified, and then notes on the run sheets the time the job started and the time it successfully completed.

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

The Scheduling Department has developed a separate set of run sheets for every date possibility. For example, a set of run sheets exists for all jobs to be executed every Thursday while a separate set of run sheets exists for jobs to be executed on only the fourth Thursday of the month. Each set of run sheets is given a Schedule Code within the application that indicates the days on which it should be printed. Based on the system date and an internal calendar, the scheduling application will match the current date to the run sheets which should be printed for that day and can produce a master list of all run sheets applicable to any given day. Should a job require scheduling on a date other than its usual run date (for instance, when the job's normal run day falls on a holiday) the Scheduler can manually add the run sheets for that job to the master list so that these run sheets will be produced with the normally scheduled set. Alternatively, if a set of nonscheduled run sheets is required immediately, the Scheduler can manually print the individual set needed. Before processing begins, the Operator checks the master list against the individual run sheets printed to ensure that he will be aware of all required jobs.

For a small number of jobs, the Operator is required to manually enter job parameters from the run sheets and start the job at his console. However, most jobs only require the Operator to initiate a Run Deck (a job stream) which already includes the required parameters for all jobs in the stream, and to note the time of start and successful completion. The run sheets include instructions for both situations.

Operators and the Operations Manager are the normal CDP personnel that perform the various operating tasks (including backups and batch processing). In peak or backup situations, operating tasks may be performed by technical staff previously trained in operational procedures, but only under the supervision of appropriate operations staff and management.

The process of adding and/or deleting jobs to/from the Run Sheet Master Lists and the run decks is initiated by the technical (programming) staff. In this process, the requested change is given to the Scheduler who makes the change and then returns the updated document to the requester.

The CDP General Manager ensures that the scheduling and operations functions are staffed by personnel with adequate job experience and expertise. Given the maturity of the systems, job abends are extremely rare. In most instances, the run sheet document indicates the restart procedures to be followed. However, should processing problems continue to occur, the Operator will contact the Operations Manager for instructions. The Operations Manager determines the scope of the problem (hardware/software) and identifies which procedure to follow or technical person to contact. The Operations Manager continues to monitor the problem until resolution. Once the problem is resolved by either arranging to have the hardware repaired or the program corrected, restart procedures are followed. Such restart procedures include:

- A. If no files are being updated, the job is restarted in its normal manner.
- B. If files are being updated, the original files are reloaded and the program is then executed from the beginning step.

So that he can be reached in an emergency, the Operations Manager carries a pager at all times.

Certain report processing for the Home Health Billing, Payroll, and Accounts Payable applications is dependent on actions taken by the user to indicate that they are ready for processing to occur. In these cases, the user will flag the report within an application screen to indicate their readiness and will notify the CDP Scheduler via electronic mail or phone that they are now ready for processing to occur.

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

The user initiates the following reports and processes:

- A. Home Health Care System:
 - 1. Pre-Billing Register
 - 2. Final billing processing and related reports

- B. Payroll System:
 - 1. Biweekly payroll process and related reports
 - 2. Month-end payroll general ledger interface and related reports

- C. Accounts Payable System:
 - 1. Weekly accounts payable checks and related reports
 - 2. A/P month-end close, general ledger interface and related reports

- D. General Ledger/Financial Reporting System:
 - 1. Allocation of indirect cost and related reports
 - 2. Revenue and expense reports (various options)
 - 3. Quarterly function report

- E. Bank Reconciliation System:
 - 1. Preliminary close (and related reports)
 - 2. Final close (and related reports)

The CDP Scheduler performs a daily inquiry of all flags to determine the validity of the flagged items and whether run sheets for additional print jobs must be added manually to the master list. Additionally, the Scheduler may respond to special requests from the users on rare occasions. These requests are normally received via electronic mail transmissions. On such requests, the Scheduler may elect to verify the contents of the request by calling the requester. This further assures that the request was truly initiated by the name displayed on the electronic mail message. The electronic mail message also carries the site and station number initiating the request. With the many years of relationships between the users and CDP personnel, the requester is normally recognized when such phone conversations take place. Although Scheduling personnel at CDP will perform some validity checks (i.e., billing month, date ranges, etc.), the final responsibility for controlling these flagging tasks and requests rests with the users.

The final task of the operator on each shift is to assure that all jobs and run sheets have been completed successfully. The Operations Manager subsequently reviews the daily processing logs to ensure that each process completed accurately and in the prescribed method. Management investigates all deviations, and all errors are referred to a project manager for correction.

The majority of application transaction posting is performed real-time, rather than under a batch process. Most of the batch processing that does occur at CDP is recurring and under the complete control and configuration of CDP, rather than specified by the user. However, certain processing and report jobs require the user to specify that they have completed all data entry and other tasks required for processing to occur. Alternatively, if the user is unprepared, they may indicate that they are not ready for the processing of these jobs to occur and have them postponed.

Should a batch processing job require rescheduling on a date other than its usual run date (for instance, when the user was not ready on the job's normal run day), Scheduling personnel can manually add the run sheets for that job to the master list so that the run sheets for the specially requested jobs will be produced in addition to the normally scheduled set. Alternatively, if a set of run sheets for specially requested jobs

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

are required immediately, Scheduling personnel can manually print the individual set needed. Before processing begins, the Operator and the Scheduler check the master list against the individual run sheets printed to ensure that the Operator will be aware of all specially requested jobs and any parameters which should be manually specified. The Operator notes on the run sheets the time the job started and the time it successfully completed. Normally, specially requested jobs will be processed from run sheets and not as part of a pre-established run deck.

Beyond data processing, certain report processing for the Home Health Billing, Payroll, and Payables applications is dependent on actions taken by the user to indicate that they are ready for processing to occur. In these cases, the user will flag the report within an application screen to indicate their readiness and will notify the CDP Scheduler via electronic mail or phone that they are now ready for processing to occur. State level personnel dictate report processing dates to CDP. Scheduling exceptions due to user sickness, vacations, etc. may occur on certain occasions and CDP handles such exceptions on a one-on-one basis with the user. Additionally, the CDP Scheduler performs a daily inquiry of all flags to determine the validity of the flagged items and whether run sheets for additional print jobs must be added manually to the master list.

A job log indicating the successful or unsuccessful completion status of each customer's processing run is produced to ensure that each job completed successfully. The Operations Manager reviews the daily processing logs to ensure that each process completed accurately and in the prescribed method. All deviations are investigated by management and all errors are referred to a project manager for correction. A complete backup, including all customer data files and report jobs, is produced prior to each processing run. Should reprocessing be required, backup tapes can be restored and processing run again.

Through the application functions, users may also request that any report for which they have authorization be printed locally at any time. Reports produced through batch processing remain available for printing until it is either overwritten during the next processing cycle for which the report job is scheduled or when it is automatically purged five days after creation.

During on-line processing, validation checks are performed to ensure that data is accurate. All errors are detected immediately and no rejects occur in subsequent processing. Each of the applications contains daily reports that show all transactions entered the prior day. Missing patient encounters are also detailed on a daily report and a daily register of all encounter activity and all assigned encounters are supplied to the user for use in tracking the missing items.

Most users of the Home Health Care System request what is referred to as a "patient pre-billing register." This is normally an overnight report displaying all visits entered by patient grouping. The user then performs a final edit against those visits residing in the patients file folder before scheduling the final billing.

The majority of CHS System application reports are automatically generated and sent to user sites during the nightly batch processing.

Reports produced through batch processing remain available for printing until it is either overwritten during the next processing cycle for which the report job is scheduled or when it is automatically purged five days after creation. Report files are backed up as part of the nightly backup process before any batch jobs are initiated and may not be archived for as long as the applicable backup tapes are available.

Alternatively, a user can manually request that a report for which he is authorized be printed at his site at any time. By viewing an "Report Inquiry by Site" screen, the user can determine which reports are still

<p style="text-align: center;">DESCRIPTION OF CONTROLS PLACED IN OPERATION Provided by Custom Data Processing, Inc.</p>

on the system at that time. The user may request a report through a simple command line entry that requires the originating site, the report number, the destination printer, and the desired pages to be printed.

The system uses printer queues to manage the printing process. This allows greater flexibility in printing reports and it removes the management of printing from CDP and places it on the user. Using print queues and the on-line report printing application (Q-Print) allows the user to print special forms at any time, monitor the progress of the printing process, route reports to alternate printers, change the form assigned to a job, and hold jobs to print later. The Q-Print print utility contains a "valid site" table that determines whether a site is authorized to print a given report. CHS program directors advise CDP's technical staff personnel as to which alternate sites are authorized to print another site's reports.

A "QSTATS" report, which lists all reports produced (either through batch or through user-initiated requests), the requesting station, the station to which the report was routed, and the size (by pages) of each report, is generated during each processing cycle. The report is available to CDP personnel only and is used for trouble shooting problems.

Ad-hoc report requests are managed under the same procedures governing changes to applications.

Physical Security

CDP Frankfort (Development; Recovery; Support)

Physical access to CDP Frankfort is controlled at several layers. The facility is surrounded on three sides by a high, chain-link fence. The fence gate remains open during the day and is padlocked at night. The front entrance to the facility, manned by a receptionist, is left unlocked during business hours but is dead bolt locked after hours. The other entrances to the facility - one in the rear of the building, one on the side of the building, and the loading dock - remain continuously dead bolt locked. CDP has installed a new electronic security system, which requires card access, as well as additional motion-detection devices.

Hardware, including all Compaq Proliant 6400 series servers and tapes are kept in the computing area. The computing area is composed of a self-contained set of rooms within the Frankfort facility. No walls of the computing area are exterior walls of the facility. The computing area is protected with raised flooring, two separate air conditioning systems, a backup power supply, and a fire extinguisher. The computing area remains unlocked during the day and is locked (standard lock) at night. CDP Network staff are normally in this area throughout the day and are observing access to the area.

CDP La Grange (Operations; System Support)

CDP La Grange is located on the top floor of a two-story office building in the business district of the town. A computer operations room, housing the Compaq Proliant 6400 series servers, communications equipment, hardware and operator documentation, backup power supply, air conditioning units, and on-site back-up tapes is completely self-contained within the CDP facility.

General physical access to the facility is controlled (1) with a key lock on the front building entrance at street level and key card lock on the second floor facility main entrance and (2) by a dead-bolt lock on the second floor rear entrance located in a stairwell to the parking garage and roof. During office hours, visitors must identify themselves to the CDP receptionist via intercom before she will electronically unlock the street entrance doors. After hours, access to the facilities is restricted to individuals with key

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

cards, which includes all CDP employees and a nightly maintenance person. Service deliveries are made in the rear of the building via an elevator, which remains positioned on the second floor until a CDP representative physically releases it to descend to the street level loading dock.

The computer operations room can be accessed from three entry points. Access to the computer operations room has been limited to a more restricted group of cardholders that have a legitimate business need for entry.

In addition to controlling access, the key card system logs each access attempt by card number and location any time a card is swiped through a reader. Should any suspicious activity require investigation, the logs would be reviewed to determine the last card used to gain access to the area where the activity occurred. The receptionist also reviews the logs daily. CDP retains the key card logs generated each day for a period of four months.

Responsibility for determining a person's key card access level rests with the General Manager. Upon his verbal instruction, the receptionist configures the key card security software to establish the appropriate access for the card. The General Manager at each CDP location is also responsible for completing the Revocation of Access Checklist to ensure that all CDP security access (physical and logical) is immediately revoked from an employee leaving the company.

The President, Vice President, Operations Manager, Administrative Assistant, and Building Owner all have keys to the rear entrance. The Receptionist also maintains a set of keys at her desk. This door remains locked except when extended access from the rear is required for building repairs, etc.

CDP maintains 24 hour/7 days per week Operations coverage throughout the year. The facilities are equipped with an alarm system which is connected electronically to an outside security company. In rare instances (i.e., Christmas day) when no Operations staff is on duty, the alarm system is activated. The alarm system monitors break-ins at entrances, and movement within the facilities. Should the system detect unauthorized access to the facilities, the system will alert the security company who will notify specified CDP personnel to take action. There is also a heat monitoring system operational 24 hours per day that monitors the temperature within the computer operations room. If the temperature within the computer operations room rises above 76 degrees Fahrenheit, the system will also alert the security company.

On-Line Security

The CDP Information Systems Security Policy communicates management's expectations regarding information security to all company personnel. This policy discusses the use of user ID's and passwords, software licensing violations, access to systems resources, access and confidentiality of data, and contingency planning. The Standards of Conduct - Confidentiality Agreement addresses the confidentiality of customer data and proprietary CDP information. All CDP personnel are given copies of both documents and are required to sign the Standards of Conduct - Confidentiality Agreement indicating that they understand and agree with both policies.

Logical access of CDP personnel to CHS application programs and data is limited to specifically authorized individuals for whom appropriate access has been systematically evaluated. All programmers at both CDP Frankfort and CDP La Grange have restricted access to all application source code and customer data files. However, the system requires the NT servers to be logged in under a common user ID to allow a Master Control Program to run. The NT servers are logged in under a system administrator

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

equivalent user ID. The NT servers are locked with a screen saver password. Several CDP employees with access to the computer operations room, including operators and programmers know the screen saver password for the production servers.

Data ownership of CHS data has been established within CHS so that specific management personnel are ultimately responsible for the accuracy and completeness of their data.

SonicWALL firewalls have been implemented in Frankfort and LaGrange, in order to secure the network.

System and application user IDs are distributed to CDP personnel (both La Grange and Frankfort) by the CDP Security Administrator based upon the requirements needed for completing one's job. Due to the infrequency of such changes, the CDP Security Administrator handles such occurrences in an informal manner. System and application access granted to CHS personnel is the responsibility of CHS. (See the User Control Considerations in Appendix B) While a few applications have additional application level access controls, logical access to applications is primarily dependent upon whether a user has been included within particular Security Groups during the setup of their user ID. On rare occasions, the CDP Security Administrator may be requested to grant a CHS user system access or may be required to assist the CHS Security Administrator perform that function. In this event, the CDP Security Administrator will validate such a request with the CHS Security Administrator to ensure that the request is authorized.

Should a CDP employee be terminated or otherwise leave the company, that user's access would be deleted immediately by the Security Administrator. The General Manager at the CDP location is responsible for notifying the Security Administrator and completing the Revocation of Access Checklist to ensure that all CDP security access is immediately revoked from the terminated employee.

CDP passwords must be a minimum of six characters in length, with at least one character being alphabetical. Passwords expire every 60 days and the same password cannot be reused for five generations. The CDP security administrator assigns users within CDP their system user IDs and a standard initial password. Upon initial sign on, the user is prompted to immediately change his/her password. While the system does not currently prompt the users to change their passwords, users do have the ability to change their password at any time. After three unsuccessful attempts to log on, a user will be logged off, but not locked out, of the system.

The Help Desk/Security Coordinator is responsible for the security function for all CHS users of CDP applications. For an employee to obtain access, a department head or the employee must contact the Security Coordinator and request access. If the Security Coordinator feels that the request is questionable, confirmation with the requesting employee's department head is obtained. In situations where the Security Coordinator is unavailable, one of three backup individuals will grant access.

System and application security are integrated functions. The Security Coordinator grants logical access by establishing a user account and setting profiles within that account. These profiles control the application level security. The user accounts are created with a naming convention (KYxxxx), and all passwords are initialized to the account names. Some users choose to change their passwords. Upon establishing an account, the Security Coordinator completes and retains a Local Health Network (LHN) Security Request Form to document to whom what access was provided.

Communications between Custom Data Processing and client sites are established using a Front End Processor (USA FEP), which is configured at CDP, to define transactions, programs, host systems, transmission channels, and security groupings. The front-end processor maps incoming transactions to the specified application and output activity to the appropriate terminal or printer. All Technical and

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

Network staff have access to modify the front-end processor routing module. A LAN router connection is used for the Jefferson County Health Department. This site accesses a Windows NT server that functions as a firewall and a terminal emulation server.

This and other front-end communications equipment are housed in an access controlled computer operations room. CDP's USA Frame Communications Processor ensures that transmissions are being sent using the TCP/IP protocol. If additional support is needed, the Help Desks will contact the CDP Frankfort facility Network Support group. USA FEP also sends a check sum with the transmission that is verified by the receiver to ensure that the transmission was received completely. Any lost frames are automatically retransmitted.

Each morning, the Operator at CDP uses the Line Status command to check the lines for protocol errors or other problems that might indicate transmission difficulties. Network Support personnel will also review the Line Status screens for the type and number of errors per line that have occurred that day. The Station Status command is utilized to determine the type and number of errors for individual stations on a particular line. Where an unusually large number of errors or a significant number of protocol errors are noted, the Network Support personnel will investigate to determine the reason.

For all report requests, a Q-STATS report lists the station number making the request, the number of pages that actually printed, and the station to which the report was sent. CDP's "On-Line Q Print Software System" is used to control this printing activity. This report is used by CDP for troubleshooting when printing problems are reported by users. Network Support personnel also monitor the PRTA Status screen to ensure the on-line status of all printers.

All of the remote sites have the ability to communicate and to share information with each other. These same sites are continuously connected to the state level help desks at the Kentucky Cabinet for Health Services as well as CDP's network support units. The on-line connectivity to the various help desks creates a feeling among the users that both state and CDP personnel are "residing" in their remote sites' environment. CDP La Grange and Frankfort network support personnel maintain a Network Problem Tracking System to record all network/communications problems either reported to them by users or detected by CDP. The tracking system includes the ability to prioritize problems, document action taken to address the problem, and to close out the problem when it has been resolved. Additionally, the tracking system generates problem-tracking reports that list problems by site and by type. These reports are reviewed weekly by Network Support personnel in order to identify any problem trends and long outstanding problems.

Sensitive system utilities are protected by the On-Line System Security Module user profile authorities and by granting transaction authority to authorized users. Customer data files are updated and maintained through programmed procedures within the applications and through scheduled nightly batch processing. For instance, the Accounts Payable and Financial Reporting System includes numerous transaction types (voids, reversals, hand checks, etc.) with all account distribution validated against the on-line chart of accounts file as each vendor transaction is entered. Additionally, the Payroll System requires all batches (including those within the verify option) to be in balance before a payroll run can be scheduled. On-line file maintenance entries are logged by the application and reported via audit trails for CHS users to review.

Levels of security are maintained by those few individuals with administrator rights to the Novell network. Separate "groups" are defined for both programmers and network staff. The individual "group" definition has associated to it all of the access rights to be assigned to the individuals in the particular

DESCRIPTION OF CONTROLS PLACED IN OPERATION
Provided by Custom Data Processing, Inc.

group. These access rights are then further refined based on an individual's needs. User identification and passwords are required to access the system.

Management and maintenance of the routers is strictly a function of the Networking staff. These routers are then password protected and only the Network staff has access to these routers.

A very limited number of key staff has access to the system remotely. These individuals generally utilize cable modems to access the system. They have to authenticate to the system through the SonicWALL Firewall and once on the system have access only to those files and systems they would normally have.

CDP has implemented a Revocation of Access Checklist, which helps to assure that once an employee leaves, all rights and permissions are removed.

Organization and Administration

Control Objective 1

Controls provide reasonable assurance that CDP policies and procedures are documented and CDP functions and responsibilities are appropriately segregated.

Tests of Operating Effectiveness Achieved

- Reviewed the organization chart for completeness, accuracy, and appropriateness to the situation to ensure segregation of duties between functional departments.
- Reviewed the organization chart noting the degree to which Networking, Programming, Operations and Customer Support functions are segregated.
- Interviewed computer operations management to determine adherence to policy, and that operators do not perform programming functions.
- Interviewed Programming management to determine adherence to policy.
- Interviewed Customer Support management to determine adherence to policy.
- Interviewed company management to determine that the service organization policies and contractual obligations between the service organization and user organization.
- Reviewed the policies and procedures of the service organization.
- Reviewed the personnel manual for inclusion of key policies.
- Interviewed company management to determine adherence to established key policies for hiring, termination, confidentiality, salary administration, performance reviews, vacation, employee benefits, and building and system security.
- Interviewed company management regarding procedures in reviewing and responding to audit reports.
- Obtained and reviewed management meeting minutes to determine the extent of over site and supervision.
- Interviewed company management to determine that CDP personnel do not input transactions or correct transactions for CHS.
- Interviewed company management to determine that references and background checks are confirmed prior to hiring new employees.
- Interviewed Programming management to determine that programmers do not perform daily operations and only implement programming changes in the CHS environment in emergency situations.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Obtained copies of IS insurance policies and noted the effective dates and related coverage, confirmed insurance policies for IS Equipment, media reconstruction, extra expense, errors and omissions, general liability, professional liability and employee dishonesty.

Software Implementation, Maintenance, and Documentation

Control Objective 2

Controls provide reasonable assurance that changes to existing systems are authorized, tested, approved, properly implemented, and documented to provide an audit trail to facilitate future program changes.

Tests of Operating Effectiveness Achieved

- Inquired of the CDP Programming Manager regarding the change request process to determine that a System Change Request Form (SCRF) is submitted by the requestor and includes a brief description of the change and the requestor's contact information.
- Inquired of the CDP Programming Manager regarding program changes for Louisville, Lexington, and Bowling Green and other non-statewide locations to determine that changes can be requested informally by authorized individuals at each location.
- Inspected a judgmental sample of SCRF's to determine that requests were authorized by CHS, a cost estimate was given by CDP and signed by the General Manager or Programming Manager, CHS approval was given to begin the program change, and CDP documentation of completion was given.
- Inspected the corresponding entry in the on-line project tracking system for a judgmental sample of program change requests to determine that each change request was entered into the tracking system.
- Inspected a judgmental sample of VDT Extract logs to determine that a copy of the log was printed and reviewed by management to ensure proper implementation of system changes. Traced the changes back to the system-generated copy of the VDT Extract logs for verification.
- Inquired of the CDP Programming Manager regarding the use of programmer documentation within a modified program and programmer preparation of user documentation.
- Inquired of the CDP Vice President, CDP General Manager, and Programming Manager to determine that programmers test the changes they make to programs prior to submitting them to the General Manager or Programming Manager for review.
- Inquired of the CDP Vice President, CDP General Manager, and CDP Programming Manager to determine management program review procedures performed prior to the implementation of a changed program.
- Inquired of the CDP Vice President, CDP General Manager, and Programming Manager to determine senior management review of change request information and status within the tracking system.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Inquired of CDP General Manager and Programming Manager to determine that if a person attempted to check out a program that had already been checked out an error message would be displayed.
- Judgmentally selected a sample of CHS financially significant executable programs and inspected the corresponding Program Implementation Request form and change requests to determine that the last change to the executable code selected was authorized by the Programming Manager or the Operations Manager.
- Inquired of the Operations Manager to determine that the Operations Scheduler uses the Program Implementation Forms to schedule movement of changed programs into the production environment each evening.
- Inquired of the Operations Manager to determine that source code is backed up prior to implementing program changes.
- Inquired of the Operations Manager to determine operator verification of program change information.
- Inquired of the Operations Manager to determine his review of daily processing logs, Program Implementation Request forms, and the system compile date for changed programs.
- Inquired of the Vice President, General Manager, and Programming Manager to determine that periodic meetings are held with CHS personnel to discuss development progress and rejected change requests.
- Inquired of the Vice President, General Manager, and Programming Manager to determine that the weekly Project Status meeting is used to discuss all outstanding projects at the La Grange location, and that the Programming Manager conducts a weekly review of all open requests at the Frankfort Location.
- Inquired of the Vice President, General Manager, and Programming Manager to determine the procedures followed for emergency fixes.
- Selected a sample of programs changed and verified that the system logs reviewed properly depicted the changes to the production code and operations management verification that a properly authorized Program Implementation Request form is maintained for the changes.

Control Objective 3

Controls provide reasonable assurance that changes to existing system software and the implementation of new system software are authorized, tested, approved, properly implemented, and documented.

Tests of Operating Effectiveness Achieved

- Discussed with management procedures for installing new system software patches and releases.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Inquired with appropriate company personnel to determine if the last version of system software patch or release was installed with management approval.
- Discussed with management the testing procedures for new system software patches or releases to help ensure the integrity of the processing environment.
- Discussed with management the extent backups are performed prior to installing system software release or patches.

Physical Security

Control Objective 4

Controls provide reasonable assurance that safeguards and/or procedures are used to protect computer equipment, storage media, and program documentation against intrusions, fire, and other hazards.

Tests of Operating Effectiveness Achieved

- Inquired of the Frankfort General Manager to determine that the door to the Frankfort facility and gate to the parking lot were locked after business hours.
- Inquired of the Frankfort General Manager to determine that a receptionist was stationed at the front entrance to Frankfort facilities during business hours.
- Inquired of the Frankfort General Manager to determine that the rear, side, and loading dock entrances to the Frankfort facility have dead-bolt locks.
- Inquired of the Frankfort General Manager to determine that the Frankfort computing area had raised flooring, two separate air conditioning systems, a backup power supply, a fire extinguisher, and that none of the walls of the computing area were exterior walls of the building.
- Inquired of the Frankfort General Manager to determine that the doors to the Frankfort computing area are locked after business hours.
- Inquired of the General Manager and Vice President to determine that the La Grange computer operations room had a backup power supply, air conditioning units, and that the computer operations room is completely self-contained within the facility.
- Inquired of the General Manager and Vice President to determine that a key lock is in place and that visitors must identify themselves to the receptionist who can then electronically unlock the door in order to enter the La Grange building from the street level entrance.
- Inquired of the General Manager and Vice President to determine physical access controls over the second floor main and rear entrances to the La Grange building.
- Inquired of the Vice President and General Manager to determine how access is restricted to the La Grange computer operations room.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Inquired of the General Manager and Vice President to determine physical access controls over the elevator in the loading area of La Grange building.
- Inquired of the General Manager and Vice President to determine the use of the Revocation of Access Checklist.
- Inquired of the General Manager to determine the process for distribution of keys to the dead bolt lock on the back entrance door.
- Inquired of the General Manager and Vice President to determine that there is security alarm system wiring on all entrance doors and heat detection monitors within the computer operations room.
- Inquired of President, Operations Manager, and General Manager to determine the security alarm system's period of activation.
- Inquired of Vice President, Operations Manager, and General Manager to determine the use of the heat monitoring system.

On-line Security

Control Objective 5

Controls provide reasonable assurance that logical access to programs and data is limited to properly authorized individuals.

Tests of Operating Effectiveness Not Achieved

Testing was not performed due to the suitability of design qualification for this control objective. Controls were not suitably designed based on the following findings:

Finding: As noted in the previous year's report, the Windows NT Security Account Manager (SAM), a file that contains all user accounts and password information, is not encrypted. Windows NT provides the capability to use strong encryption techniques to increase protection of account password information stored in the registry by the SAM. We recommend the Windows NT SAM file be encrypted using the 'SYSKEY' function. More information about the SYSKEY function can be found at <http://support.microsoft.com/>.

Management Response: *CDP will further investigate encrypting this file. Warnings associated with Microsoft's instructions on how to implement this function make us concerned and we will tread slowly on this item – but will continue to examine it.*

Finding: An analysis of the NetWare password requirements on CDP's NetWare network identified one administrator-equivalent account with a blank password. The account is configured with rights over everything stored on the NetWare servers including documents, databases, and source code. CDP should configure every account, especially those with administrator access, to

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

require a strong password. A strong password is at least seven characters long consisting of numbers, letters, and special characters.

Management Response: The administrator account with a blank password was removed as soon as it was identified. CDP, as stated previously, is looking at strengthening our password rules where possible. Please note that CDP is moving away from the use of Novell as a valid operating system.

Finding: As noted in the previous year's report, passwords for accounts on the Windows NT and Novell (NetWare) network are required to be a minimum length of six characters and passwords are required to change every 60 days. However, current CDP guidelines do not include guidance on selecting and using strong passwords. Strong passwords typically consist of non-dictionary words including upper and lower case characters, special characters and numbers, and it must be of a sufficient length. Without the use of strong passwords, unauthorized access to the network may be gained. We recommend that passwords for the NetWare and Windows NT network be required to be a minimum of seven characters in length. In addition, we recommend enabling the password change frequency option to require users change their passwords every 45 days to increase the security over user accounts. Finally, we encourage management to educate users on selecting and using strong passwords.

Also, we sampled seven accounts on the NetWare network to validate that passwords controls are in compliance with documented CDP standards. Five of the seven sampled accounts were not in compliance with these standards. We recommend that CDP management emphasize to their users the importance of adhering to corporate standards to maintain strong system passwords.

Management Response: On CDP accounts we are changing the password to be longer (a minimum of eight characters) and we will also require the inclusion of numeric digits within the password. Also, where possible, we will require that the password be changed every 45 days. It should be noted that CDP intends to move away from Novell Netware as an operating system. This will eliminate the need to have Netware logins and passwords.

Finding: As noted in the previous year's report, CDP uses USA's Front End Processor (FEP) software to connect application users to the production application servers. The FEP assigns application access to the workstations by the terminals login capability, log off capability and by individual user ID access. While CDP personnel complete the initial setup of end user workstations to the FEP, the user is ultimately responsible for setting access levels assigned to each individual. The log off capability for each workstation through the FEP is a reserved access type. A workstation that allows log off capability to certain security codes could allow anyone with physical access to the workstation to enter transactions authorized under the log off capability without entering a user ID or password. Only CDP employees have access to change this level of security settings. In addition, terminal setting changes are not logged. Finally, several CDP employees are responsible for administrating the FEP security. These employees share a single login to make security changes. To provide accountability for each user's actions on the system, we recommend that all users have their own unique account names and passwords.

Further, as noted in the previous year's report, the FEP user account password is not encrypted during transmission across the internal CDP network. We encourage CDP to investigate encryption options for all FEP passwords transmitted across network traffic.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

Management Response: It should be noted that CHS actually is ultimately responsible for setting access rights to the system. CDP staff actually only define the users as being in existence. Also, no stations are allowed to have “log off” capabilities; this is monitored on a weekly basis. We are still awaiting CHS approval of modifications to the USA FEP software to enable the logging of transactions.

Due to the USA FEP security/user structure/rules, only the administrator account that built an individual user can also maintain it. Consequently, there may be occasion when more than one individual may need to know an account password. There are only a select number of individuals that have this capability.

CDP has investigated encrypting passwords over the network and it would be a costly change from the software vendor. With the fact that the end user must first sign on to the Checkpoint firewall, which uses encryption, the only place that the encryption does not occur is on the internal CDP network. We will continue to study how this might be accomplished with hardware strategically placed within our network.

In addition, although issues and risks concerning the viewing of unencrypted information once access is acquired to the internal network remain as a concern, external access by individuals would require that each intruder obtain Bridge software, all the configuration information for the client and the Multi-Bridge server information. Additionally, they would have to come from a valid computer site number for the Hid/Loc/S they were trying to access. The intruder would also have to be a valid user that signed onto the PES system over and above signing onto the FEP as a valid user and password. Finally, they would also still have to authenticate to the Checkpoint VPN server to gain access to the Multi-Bridge server. Given the cost of the encryption software (estimated at \$40,000) and the described procedures that are now in place for responding to unauthorized intrusions, we believe that the risk obtaining clear text passwords and information from outside is low and that the expense far out weighs the benefits of this additional control.

Finding: While CDP has implemented firewalls to help secure the internal network, the publicly accessible web server is not located in a demilitarized zone (DMZ). Management should consider moving this web server into a DMZ in order to better protect the network against attacks.

Also, we encourage CDP to investigate adding an Intrusion Detection System (IDS) to the CDP network. An IDS will warn administrators of events taking place on the network that could be the result of a possible attack.

Further, we recommend that CDP have periodic security assessments of the CDP network performed. Security assessments at a minimum should include:

- A review of the CDP network security strengths and vulnerabilities of CDP systems and Internet connectivity, and
- External penetration assessment that verifies CDP’s network has a properly secured Internet connection and publicly accessible web servers.

Management Response: CDP is testing the use of the DMZ port on the SonicWALL firewalls and is evaluating its effect on the network. We plan to implement this where possible in the near future.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

CDP has purchased software to aid in the self-examination of the network. This software is called Languard and is being used on a daily basis.

CDP networking staff is looking into the procurement of an Intrusion Detection System.

CDP management has authorized the procurement of services from a firm that performs security assessments.

Computer Operations

Control Objective 6

Controls provide reasonable assurance that processing is scheduled appropriately and deviations are identified and resolved.

Tests of Operating Effectiveness Achieved

- Inquired of the General Manager to determine the extent of regularly scheduled jobs versus specially requested jobs.
- Inspected a judgmental sample of run sheets to determine that they were appropriately produced for the day scheduled, completed by the operator, and reviewed by the operations manager.
- Inquired of the General Manager and Scheduler to determine how changes to the Run Sheet Master Lists and run decks are initiated.
- Inquired of the General Manager and Operations Manager to determine the staffing and skill level of operations personnel.
- Inquired of the Operations Manager and General Manager to determine the escalation procedures when operator restart procedures are ineffective.
- Inquired of the Operations Manager to determine restart procedures for abends occurring both during file update, and when no update is occurring.
- Inquired of the General Manager to determine who has access to the scheduling application.
- Inquired of the CDP La Grange Operations Manager to determine his review of the prior evening's processing log for abends, deviations from expected results, or other unusual items.
- Inquired of the CDP La Grange Operations Manager to determine the course of action should a deviation be discovered in the processing logs.
- Inquired of the Operations Manager to determine the pre-processing review of the master job list.
- Inquired of the General Manager to determine internal use of the QSTATS report.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Discussed with appropriate company personnel that the FEP: directs traffic and messages; auto detects communication status; uses a checksum to ensure a complete message is received; and produces a report showing line status.
- Inquired of appropriate company personnel regarding the completion of backups of company data prior to the nightly processing.
- Discussed with management the validation checks performed by the system during the nightly update to ensure complete and accurate processing.

Control Objective 7

Controls provide reasonable assurance of continued operations in the event that systems become unavailable.

Tests of Operating Effectiveness Achieved

- Observed backup hardware located at the Frankfort facility is stored on a raised floor in a climate-controlled room. Discussed the appropriate service level provided by the backup hardware of the Frankfort General Manager to determine that sufficient resources are available in the event of a disaster. .
- Inquired of the General Manager to determine functionality of the electricity-monitoring unit at the Frankfort facility.
- Inquired of the Frankfort General Manager that operating system and utility software user documentation is available at the Frankfort facility.
- Inquired of the Operations Manager and Vice President to determine that heat detection units are throughout the La Grange facility.
- Inquired of the Operations Manager to determine that the La Grange facility is equipped with a building wide sprinkler system.
- Inquired of the Operations Manager to determine the automatic notification of a security company in the event fire is detected.
- Inquired of the Operations Manager to determine that fire extinguishers are located throughout the La Grange facility.
- Inquired of the Operations Manager to determine that several functioning, self-monitoring air conditioning units are assigned to the La Grange computer operations room.
- Inquired of the Operations Manager to determine that a functioning backup air conditioning unit is located within the La Grange computer operations room.
- Inquired of the Operations Manager to determine that an Uninterruptable Power Supply (UPS) unit equipped with a battery level meter is located within the La Grange computer operations room.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Inquired of the General Manager to determine specifications for the UPS.
- Discussed periodic testing procedures for the UPS and generator for the La Grange facility.
- Inspected shutdown procedures to be used in the event of a power outage.
- Inquired of the Operations Manager to determine that a gas-powered generator is located behind the La Grange facility.
- Inquired of the Operations Manager to determine the tape vault within the La Grange computer operations room contained backup tapes in locked cases for the third and fourth most recent processing days.
- Inspected the backup tape off-site storage agreement.
- For tapes returning from off-site storage, reloaded one tape returned to ensure the tape was readable and contained the information indicated, inventoried the tapes in the case returned from off-site storage to ensure all appropriate tapes are accounted for and were properly taken to the off-site facility for the day tested.
- Inquired of the Operations Manager to determine that the tape vault within the CDP La Grange computer operations room housed tapes for the previous month's systems resource pack and tapes for executable code from the previous five days.
- Inquired of the Programming Manager to determine that a duplicate copy of archived data from the PES Patient Purge, History Purge, and Appointment Purge was housed in the Frankfort tape room.
- Inspected the Business Resumption Plan notebook kept at the Frankfort site to determine the following were included in the plan:
 - instructional overview and delineation of team responsibilities
 - USAFEP Restore Instructions
 - CDP personnel names, addresses and phone numbers
 - vendor contact phone numbers
 - checklist of chronologically ordered procedures to be performed in the event of a disaster for all systems
 - detailed instructions covering the sequence and names of tapes to load and system start-up procedures
 - hub site contact lists
 - priority schedules
- Inquired of the Frankfort General Manager to determine the use of the Kentucky user's bulletin board.
- Inquired of the General Manager to determine whether backup hardware had been used/tested during the period.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Inquired of the CDP La Grange General Manager to determine whether the Business Resumption Plan had been tested.
- Inquired of CDP General Manager to determine the protocol for the switching of communication lines in the event of a disaster.
- Inspected the documented test results summary from the most recent disaster recovery test.

Control Objective 8

Controls provide reasonable assurance that system and application backup procedures are performed; significant files are stored off-site; and formal plan for recovery have been considered.

Tests of Operating Effectiveness Achieved

- Discussed with management procedures for creating backups of data, system development and application programs and rotating the backup tapes to off-site storage.
- Determined that the procedures used to take backup tapes off-site result in an adequate rotation schedule.
- Reviewed a sample of backup logs and verified that the checklists were present and complete.

Control Objective 9

Controls provide reasonable assurance that output data and documents are distributed to authorized recipients on a timely basis.

Tests of Operating Effectiveness Achieved

- Inquired of the Systems Manager and Network Support personnel to determine the procedures involved when a customer station is not available to receive data transmissions.
- Inquired of the Systems Manager to determine the use of the Line Status command to check the lines for protocol errors or other problems.
- Inquired of the Systems Manager to determine the use of the Station Status command to check for errors on a particular line.
- Inspected the PRTA Status screen to determine an indication of all printer sites and their current on-line status.
- Inquired of the Systems Manager and Network Support personnel to determine the course of action when transmission errors are detected.
- Inquired of Network Support personnel to determine the weekly monitoring of problem tracking reports for unusual items and problem trends.

APPENDIX A – TEST OF OPERATING EFFECTIVENESS

- Inquired of Scheduler to determine user actions required to print reports.
- Inquired of Scheduler to determine CDP's on-line inquiry of the applications for user-flagged reports.
- Discussed procedures for users to submit special requests.
- Inquired of the Scheduler to determine CDP's procedures for validating the authority of the requestor for special requests.
- Inquired of the Operations Manager to determine if an electronic mail is delivered to the Scheduler from a user at CHS requesting a special report run.
- Inquired of General Manager regarding length of time for which report files were accessible.
- Inquired of the Systems Manager to determine access to files in the print queue.
- Inquired of the System Manager to determine the use of the Q-Print utility to print customer reports at the La Grange site.
- Inquired of the Systems Manager to determine the process by which one customer site authorizes a report to be printed at another site noting that authorization is granted in writing by the CHS program Directors.
- Inquired with company management regarding the availability of reports after nightly processing and the request procedure to have reports remote printed to various CHS locations.

USER CONTROL CONSIDERATIONS

This section outlines specific user control considerations, or issues each agency may want to consider and address for the purpose of monitoring the data processing done by CDP. These considerations are not necessarily a comprehensive list of all internal accounting controls that should be employed by the user agency, nor do they represent procedures that may be necessary in all circumstances.

Organization and Administration

- CHS should develop policies and procedures regarding the use of the CDP applications.

Disaster and Contingency Planning

- Controls should be established to ensure that information can be reentered into the system from source documents for a period of 48 hours.
- Controls should be established to ensure that in the event of a disaster at CDP, workflow arrangements will not be significantly impeded in the event access to the CDP provided application systems is not available for 48 hours.
- CHS should develop a contingency plan considering the CDP contingency planning provisions.

Software Implementation, Maintenance, and Documentation

- Controls should be established to ensure that CHS management communicates on a timely basis to users when a program change has occurred

Computer Operations

- Controls should be established to ensure that balancing of application reports and inspection of application data files is performed to discover incomplete or inaccurate data transmissions.
- Controls should be established to ensure that processing parameters are initially entered accurately by the customer.
- Controls should be established to ensure that changes to processing parameters are reviewed for appropriateness by authorized personnel at the customer sites.
- Controls should be established to ensure that all file maintenance transactions and user audit trails are reviewed to ensure changes are authorized, complete, and accurate.
- Controls should be established to ensure that all reports created for a user and added to the print queue are actually printed.
- Controls should be established for requesting special processing requests to ensure that requests are appropriately approved.

APPENDIX B –USER CONTROL CONSIDERATIONS

- Controls should be established for communicating when run jobs are authorized to be completed or when they need to be delayed.
- Although Scheduling personnel at CDP will perform some validity checks (i.e., billing month, date ranges, etc.), the final responsibility for controlling these flagging tasks and requests rests with the users.
- Controls should be established to ensure that only authorized user personnel have the ability to flag reports for processing by CDP.
- Controls should be established to ensure that user-scheduling requests are made at appropriate times and that all elements of the request are valid.
- Controls should be established to ensure that balancing of application reports and inspection of application data files is performed to discover incomplete or inaccurate data transmissions.
- Controls should be established to ensure that users review the report printing schedule checklist to verify printing schedules.

Physical Security

- Controls should be established to ensure that physical access is observed over the security of reports containing sensitive or private information and devices connected to CDP.

On-Line Security

- Controls should be established to ensure that CHS user access is commensurate with the user's job requirements.
- Controls should be established to ensure that initial requests for CHS user access and requests for changes to user access are appropriately authorized.
- Controls should be established to ensure that all additions, deletions, and/or changes to user access made by CDP on behalf of, or in conjunction with, CHS are authorized and accurate.
- Controls should be established to ensure that terminals are not left logged in and unattended, allowing an otherwise unauthorized person from accessing restricted information or requesting special processing requests to CDP.
- Controls should be established to ensure that any additions, changes, or deletions of CHS users are communicated to the CHS Security Administrator in a timely manner and that user access within CHS applications is commensurate with job responsibilities.

APPENDIX C – ORGANIZATION CHART

CUSTOM DATA PROCESSING, INC.
Organizational Chart - 2002

