H. CARL McCALL
STATE COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

November 26, 2002

Antonia C. Novello, M.D., M.P.H., Dr. P.H.
Commissioner
Department of Health
Corning Tower
Empire State Plaza
Albany, NY 12237

Re: Health Care Initiatives Pool
Disbursements
Report 2001-S-43

Dear Dr. Novello:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law, we have audited the Department of Health's (Department) oversight of Health Care Initiatives Pool disbursements. Our audit assessed the Department's oversight activities for the period January 1, 1999 through March 31, 2002.

A. Background

The Health Care Reform Act (HCRA) of 1996 established three pools – Indigent Care, Health Care Initiatives and Professional Education – to fund public goods. In December 1999, the Legislature passed HCRA 2000, which extended many of the provisions contained in the original HCRA through June 30, 2003. The Health Care Initiatives Pool (HCI Pool) was established to fund various programs administered by the Department of Health (Department). HCRA amended New York State's Public Health Law by adding section 2807-L, which stipulates how the Department must distribute the funding available in the HCI Pool. Specifically, HCRA identified 27 Department programs that are eligible to receive funding from the HCI Pool along with the maximum amount each of these programs can receive each pool year.

The Department disburses HCI Pool funds to eligible programs in accordance with an appropriation or directly from the HCI Pool (off-budget). After the Legislature approves a program's annual appropriation, the Office of the State Comptroller (OSC) monitors and pre-approves all payments the Department makes against that appropriation. Payments the Department makes to off-budget programs undergo a Departmental review and approval process, but the Department does not need to seek prior approval from OSC before making related payments. Of the

27 programs to which HCRA allocated HCI Pool funding, 21 programs are off-budget. Since HCI Pool funding ended for 5 of these programs when HCRA of 1996 expired, our audit focused on the 16 programs that continue to receive off-budget funding. The Department disburses the majority of off-budget HCI Pool funding to providers according to the terms of executed contracts or formulaic percentages of available funds for a Department program. Department records show that, as of August 24, 2001, the Department disbursed HCI Pool funds totaling $115 million and $91 million, respectively, in calendar years 1999 and 2000, to the 16 off-budget programs or individual contractors.

The Department delegates responsibility for administering the HCI Pool to Excellus Health Plan Incorporated (Excellus), formerly known as Blue Cross and Blue Shield of Central New York. The Department's contract with Excellus gives Excellus the responsibility of collecting, administering and distributing the funds in the HCI Pool in accordance with Department directives and HCRA. Excellus has assumed these responsibilities since HCRA created the HCI Pool in 1996.

B. Audit Scope, Objectives and Methodology

We audited the Department's oversight of HCI Pool disbursements (off-budget funds) for the period January 1, 1999 through March 31, 2002. The objectives of this financial-related audit were to determine whether the Department (1) has established controls over HCI Pool disbursements to provide reasonable assurance that off-budget disbursements are calculated accurately, recorded correctly and made in conformance with HCRA requirements; (2) executes HCI Pool contracts in a timely fashion; and (3) effectively oversees Excellus' administration of HCI Pool funds, including the adequacy of the automated systems Excellus uses to track and report HCI Pool activity.

To accomplish our objectives, we interviewed Department officials, reviewed applicable sections of HCRA and examined the Department's policies and procedures pertaining to the HCI Pool. In addition, we visited Excellus to determine whether it maintains sufficient controls over the automated system it maintains for tracking HCI Pool activity. To assess the level of compliance with applicable Department policies and HCRA legislation, we selected a random sample of 20 out of 311 contracts that were in effect during the 1999 calendar year and 20 out of 423 contracts that were in effect during the 2000 calendar year. Our objective was to determine whether contracts were properly approved, whether payments were properly calculated and made in accordance with contract provisions, and whether payments were accurately captured on Excellus' accounting systems. We also selected a random sample of 30 out of 1,111 HCI Pool disbursements that Excellus made during the 1999 calendar year and 30 out of 1,198 HCI Pool disbursements that Excellus made during the 2000 calendar year to determine whether the Department had approved the disbursements. In addition, using computer assisted auditing techniques, we analyzed all disbursements listed on Excellus' database for 1999 and 2000 pool years for evidence of duplicate payments and incorrect recording of disbursements.

Despite our numerous requests over a four-month period, Department officials did not provide all of the documentation we requested for our audit. Specifically, Department officials provided only 28 of the 40 contracts we requested and provided complete documentation for only 21 of the 60 disbursements we requested. As a result, we were unable to complete our assessment of the Department's controls over HCI Pool disbursements. We consider the Department's failure to

provide us with all requested records to be a limitation on the scope of our audit. Therefore, readers of this report should consider the effect of this scope limitation on the findings and conclusions presented in this report.

Except for the effect of the scope limitation discussed in the preceding paragraph, we conducted our audit in accordance with generally accepted government auditing standards. Such standards require that we plan and perform our audit to adequately assess those Department and Excellus operations that are within our audit scope. Further, these standards require that we understand the Department's and Excellus' respective internal control structures and compliance with those laws, rules and regulations that are relevant to the operations included in our audit scope. An audit includes examining, on a test basis, evidence supporting transactions recorded in the accounting and operating records, and applying such other auditing procedures as we consider necessary in the circumstances. An audit also includes assessing the estimates, judgments and decisions made by management. We believe our audit provides a reasonable basis for our findings, conclusions and recommendations.

We use a risk-based approach when selecting activities to be audited. This approach focuses our audit efforts on those activities we have identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, we use our finite audit resources to identify where and how improvements can be made. Thus, we devote little effort to reviewing operations that may be relatively efficient or effective. As a result, we prepare our audit reports on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address activities that may be functioning properly.

C. Internal Control and Compliance Summary

Our evaluation of the internal control structure at the Department and at Excellus identified internal control weaknesses over HCI Pool disbursements, the contract approval process and Excellus' automated systems. As a result of these deficiencies, there is a risk that inappropriate payments of HCI Pool funds could be made without detection, that delays in contract approval could impact program delivery and that HCI Pool data could be accessed inappropriately or jeopardized in the event of disaster. These matters are presented throughout this report.

D. Results of Audit

Since it depends on Excellus for Pool administration functions, the Department should have adequate controls in place to minimize the risk that Excellus' disbursements are inaccurate or unauthorized. Due to the Department's failure to provide us with much of the documentation we requested for our audit tests, we cannot fully conclude on the adequacy and accuracy of HCI Pool disbursements. Based on the documentation the Department did provide, we found disbursements were generally accurate and authorized, except as noted in our report. To strengthen controls over disbursements, the Department should improve its monitoring processes to identify discrepancies between what the Department requests and what Excellus records and issues, and strengthen its authorization requirements to reduce the risk of unauthorized disbursements. The Department also needs to make sure contracts are approved before contractors perform services.

The Department also needs assurance of the integrity and security of HCI Pool data. We found Excellus has established good general and application controls, particularly in areas where the Department has provided specific guidelines and network requirements. However, the Department has not provided Excellus with adequate written policies in the areas of logical security, physical access, and business, contingency and disaster recovery plans, and improvements are needed in each of these areas.

1. Department Controls Over HCI Pool Disbursements

To determine whether the Department's review and approval process provides adequate accountability for HCI Pool funds paid for off-budget programs, we examined the accuracy of disbursements made to eligible programs under contract with the Department as well as to providers that receive formulaic disbursements of HCI Pool funds available for specific Department programs. We then assessed the adequacy of the Department's review and approval of disbursements, and its methods of monitoring Excellus to detect discrepancies between what the Department approves for payment and what Excellus records on the HCRA Pools database and disburses to payees. We also examined HCI Pool-funded contracts to determine whether they were fully approved before the contract start date.

a. Accuracy of Payments

To receive reimbursement for contract-related expenses, a contractor must submit a voucher and an expense report to the Department. To determine whether disbursements matched contactors' reported expenses, we planned to recalculate the expenses reportedly incurred and compare the result to the amount of the voucher for a random sample of 40 contracts. However, the Department provided only 28 contracts for our review, and only 19 of that number included expense reports to support vouchered expenses. We found no instances in which a voucher amount did not match reported expenses in these 19 contracts. However, expense documentation should have been present for all 28 contracts.

Of the Department's 16 off-budget programs, 3 receive funding through formulaic distributions. We concentrated our audit efforts on the highest-funded of these programs, the Diagnostic and Treatment Centers for Uncompensated Care (D&TC), which received approximately $41.6 million and $44.3 million in 1999 and 2000, respectively. A D&TC must provide at least 5 percent of its services to individuals who cannot pay for them to qualify for funds, and must report monthly to the Department on its level of uncompensated care to receive funds. The program's formula provides more funding to those D&TC entities that provide a greater share of uncompensated care.

We tested the mathematical accuracy of distributions made to D&TCs and did not identify any errors in the calculation and distribution of 1999 D&TC funds. However, we identified one provider that received a total of $488,485 in 2000 D&TC funds in error. This provider was eligible for funding in 1999, but was not a participating provider in 2000. Since qualifying D&TCs share all available program funds in a given year, this error resulted in other entities receiving less funding than they were entitled to receive for 2000. Subsequent to receiving our preliminary audit findings, Department officials stated they recovered these funds in April 2002 and will redistribute them to

entitled providers in the next distribution cycle. Department officials further stated that they are implementing steps to prevent this type of error from occurring in the future.

b. Department Approval of Off-Budget Disbursements

According to Department officials, the relevant Department Program Directors must approve all disbursements (besides formulaic distributions) to their program recipients before the payment is made. The approval process includes the Director's verification of eligibility for funding and the amount of funds, and various approvals by six officials within the Department's Bureau of Financial Management and Information Support (BFMIS). Officials stated that each individual documents his or her approval on a buckslip attached to the disbursement's payment package.

To test the Department's adherence to this policy, we used auditing software to select a sample of 60 HCI Pool disbursements reportedly made in 1999 and 2000. We asked for a copy of the buckslip, or any other evidence of Department approval, for each of these 60 disbursements. As of March 20, 2002, the Department provided adequate documentation to show that 21 of the 60 disbursements were fully approved. Of the remaining 39, the Department provided incomplete approval documentation for 2 disbursements and no approval documentation at all for 37 disbursements. Without documentation of Department approval, there is increased risk that payments could be made for incorrect amounts or to entities that are not entitled to HCI Pool funds.

c. Excellus' Recording and Payment of Disbursements

After the Department approves a disbursement, BFMIS records the transaction as a payment in progress, and sends the payment package to Excellus authorizing payment. Each payment package has a unique requisition number and contains payment information (i.e., payee name, payment amount, payment address, program and pool year). According to Excellus officials, Excellus reviews payment package information for consistency, confirms that adequate funding is available in the HCI Pool, verifies and records payment information on the HCRA Pools database and issues the payment.

To monitor the accuracy of Excellus' recording and its issuance of disbursements, the Department requires Excellus to submit monthly HCI Pool reports that list the total amount Excellus paid to each program by Pool year as well as the details of each individual disbursement. BFMIS staff reconcile the total amount (excluding formulaic distributions) Excellus reportedly paid to each program and payee against their records. If a payment reconciles, BFMIS staff change the status of the payment from a payment in process to a disbursement.

To test the effectiveness of the Department's reconciliation process, we compared payment information (payee name, payment amount, etc.) listed in the payment package with what Excellus recorded on the HCRA Pools database for a total of 83 disbursements: 55 of the 60 transactions (5 had inadequate documentation for this test) selected for our review of the approval process, and one voucher from each of the 28 contracts we reviewed for our accuracy test. The Department did not provide enough documentation to review 9 of the 83 disbursements. Our review of the remaining 74 transactions showed there were discrepancies (payee name [1], payee address [2] and requisition number [1]) between Department and Excellus data in 4 disbursements.

In an additional test, we used auditing software to examine what Excellus officials reported to be the entire Excellus' download of 1999 and 2000 HCI Pool transactions. After performing selected analyses of this data, we identified another 141 disbursements that appeared to be instances of either incorrect recording or duplicate payment. The Department and Excellus resolved our questions about all but 18 of these disbursements, each of which contained a discrepancy in payment information, such as payee name or payee address. We also identified a payment of $166,374 that was a duplicate of a previous disbursement. Department officials said this payment was issued as a replacement check, but that the payee, who finally cashed the original check, repaid the amount after having been notified of the overpayment by the Department. Although the payment information discrepancies (e.g., incorrect payee address) our audit tests identified were easily corrected, the Department's method of monitoring Excellus does not routinely identify such errors, with the result that the Department could send a check to wrong address and not know it. Further, since the Department's reconciliation process did not identify the $166,374 duplicate payment, this process needs to be strengthened to reduce the risk that overpayments will occur and not be detected.

d. Contracts

A contractor who receives HCI Pool funds must have an executed contract to legally provide services and claim reimbursement for related expenses. However, when we examined the 28 contracts used in our earlier tests, we found that none were fully approved (by the contractor, the Department, the Attorney General and OSC) until after their start date; 7 contracts were not fully approved until after the end of the contract period. We determined that delays are a result of the Department's late initiation of the approval process. The Department did not initiate the approval process until an average of 249 days after the contract start date, whereas the approval process itself took an average of only 54 days. Late approval could adversely impact recipients of services if a contractor delays or does not complete planned activities until reimbursement for services is certain.

2. Controls Over Excellus' Automated Systems

As the administrator of HCI Pool funds, Excellus records payment information and disburses HCI Pool funds based on the data on its automated systems. Since Excellus and the Department depend on the integrity of this data to make appropriate payments, it is essential that Excellus effectively control logical access to these systems, establish adequate physical security over hardware and develop business contingency/disaster recovery plans. Logical access controls and logical security controls prevent or detect unauthorized access by requiring user identification numbers and passwords and by restricting access to specific data or resources. Physical security controls restrict physical access to the server room and desktop computers at workstations and provide for eliminating sensitive data from equipment before its disposal. Excellus also needs to develop business contingency/disaster recovery plans to protect information resources, to minimize the risk of unplanned interruptions and to provide for the recovery of critical operations if interruptions do occur. We found weaknesses in the above controls over Excellus' automated systems, and recommend that the Department and Excellus act promptly to strengthen controls.

a. Logical Access and Logical Security Controls

Logical access controls involve computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers, passwords or other identifiers that predetermine access privileges. Logical security controls restrict access to specific data or resources, track user activity, take defensive measures against intrusion and identify users and computers authorized to access networks, data and resources. We found weaknesses in Excellus' controls over logical security, as described below. To address these weaknesses, Excellus should enable or maximize security settings and features intended to reduce the risk of unauthorized access.

- Password Security. The system is not designed to log-out users after excessive idle time or to use screensavers to hide sensitive data. The system also allows concurrent log-ons. Some password restrictions and account lockout settings did not meet standards stated in the systems operations manual.
- Log-in Scripts and System Documentation. Log-in scripts, which are used to automate a variety of tasks when a user logs in, should be stored encrypted to enhance security. Excellus had not encrypted log-in scripts. Further, Excellus had not documented changes to the system, an important step in creating an audit trail.
- Administrator Account. The Administrator Account, which has complete control over the system's operation and security, had not been renamed to obscure its identity from unauthorized users.
- Legal Notice. Excellus does not display a banner legal notice at log-in to warn that only authorized users may access the system, and that system use is monitored.

b. Controls Over Physical Access

Physical access controls restrict access to the computer/server room, workstations and network access points. The goals of physical security include preventing unauthorized access to system resources and protecting people, data, systems and facilities from harm. To meet these goals, Excellus needs to improve controls over server room access, strengthen physical security at workstations and develop procedures regarding the removal of sensitive data from equipment before it is retired. We detail the weaknesses in Excellus' physical security below.

- Server Room Access. Restricting access to the server room is critical to a secure computing environment. Although Excellus uses a standard lock and key to limit access to this room, electronic key cards and push-button cipher locks enhance convenience and also provide a log of user access. Written access logs were not maintained.
- Physical Security at Workstations. Floppy disks and drives present security risks, since they permit unauthorized access to the workstation's hard drive, unauthorized copying and removal of data and the introduction of viruses. Although Excellus policy states that users should not boot from a floppy drive, workstation floppy drives are not completely disabled.
- Clearing Sensitive Data from Equipment Prior to Disposal. Excellus should have procedures that require sensitive data and software to be removed from computers when they are retired from use, and should clearly assign that responsibility. Although Excellus states that it follows this practice, the Department has not provided Excellus with written procedures that require data removal and documentation of the removal process.

c. Business Contingency/Disaster Recovery Plans

Losing the capacity to process, retrieve and protect information maintained electronically can significantly affect an organization's ability to accomplish its mission. For this reason, the Department should have procedures in place to protect information resources, to minimize the risk of unplanned interruptions and to recover critical operations should interruptions occur. This plan should consider the activities performed at data processing centers and telecommunications facilities, as well as those performed by users of specific applications. Remote backup facilities and access to an uninterrupted power source can also minimize disruption to operations. We identified weaknesses in Excellus' business contingency/disaster recovery plans, backup provisions and environmental controls, as described below.

- Business Contingency and Disaster Recovery Planning. An effective business continuity/disaster recovery plan (plan) should provide for operational continuity in the event of both minor disruptions and major disasters. The plan should be thoroughly documented and periodically tested through simulation exercises to identify and correct weaknesses. Since Excellus has not completely documented and tested its plan, the Department does not have assurance of continuity and data integrity if a disaster occurs.
- Backup and Environmental Controls. Excellus should identify backup facilities that can be used if the entity's usual facilities are damaged beyond use. Since Excellus' first choice for a backup site is a location adjacent to its own building, this site could well be impacted by disaster damage; Excellus' alternate site is not documented in its plan. Further, Excellus has not installed a waterless fire suppression system or an uninterrupted power supply to keep the network running during a power failure. We also found current versions of Excellus' operating system and software was not available off-site.

Recommendations

1. *Establish and enforce compliance with formal policies and procedures for verifying the legitimacy and accuracy of HCI Pool disbursements. At a minimum, the Department should:*

    - *Require that disbursements contain sufficient documentation to support the expense;*
    - *improve the controls over formulaic HCI Pool disbursements to minimize the risk that payments will be made to providers who are not entitled to funding;*
    - *obtain and document the necessary Department approvals for disbursements; and*
    - *improve the reconciliation process to detect errors in payment information, missing authorizations and potential duplicate payments.*

2. *Make sure each contract is fully approved before its intended start date.*

3. *Require Excellus to improve controls over its automated systems by:*

- *Strengthening logical security by optimizing logical security settings and features; renaming the Administrator Account; posting a legal notice about the system's proprietary nature at log-in; and properly documenting all system changes.*
- *Enhancing physical security by using electronic key cards and logging access to the server room; disabling floppy drives at workstations; and clearing sensitive data and software from equipment before retiring it.*
- *Upgrading its Business Continuity/Disaster Recovery Plan, including fully documenting and annually testing its plan's effectiveness through disaster and recovery simulation exercises; identifying a sufficiently remote alternate disaster recovery site; installing adequate environmental controls; and keeping a current version of Excellus' operating system at the remote site.*

We provided draft copies of this report to Department officials for their review and comment. We considered the Department's comments in preparing this report and included the comments as Appendix A. We interpret the Department's comments to generally agree with our recommendations.

Within 90 days after the final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the New York State Department of Health shall report to the Governor, the State Comptroller and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons therefor.

Major contributors to this report were Ed Durocher, Kristee Iacobucci, Dennis Graves, Timothy Marten, Mary Roylance and Nancy Varley.

We wish to thank the management and staff of the Department of Health and Excellus Health Plan Incorporated for the courtesies and cooperation extended to our auditors during this audit.

Very truly yours,

Kevin M. McClune
Audit Director

cc: Deirdre A. Taylor

STATE OF NEW YORK
DEPARTMENT OF HEALTH
Corning Tower The Governor Nelson A. Rockefeller Empire State Plaza Albany, New York 12237

Antonia C. Novello, M.D., M.P.H., Dr.P.H.
Commissioner

Dennis P. Whalen
Executive Deputy Commissioner

October 17, 2002

Kevin M. McClune
Audit Director
Office of the State Comptroller
110 State Street
Albany, New York 12236

Dear Mr. McClune:

Enclosed are the Department of Health's comments on the Office of the State Comptroller's draft audit report 2001-S-43, entitled "Health Care Initiatives Pool Disbursements".

Thank you for the opportunity to comment.

Sincerely,

Dennis P. Whalen
Executive Deputy Commissioner

Enclosure

Appendix A

cc: Ms. Anderson
Mr. Angerami
Mr. Cullen
Mr. Hinckley
Mr. Howe
Mr. Malecki
Mr. Norton
Mr. Osten
Mr. Pellegrini
Mr. Reed
Ms. Taylor

Department of Health
Comments on the
Office of the State Comptroller's
Draft Audit Report
2001-S-43 Entitled
"Health Care Initiatives Pool Disbursements"

The following are the Department of Health's (DOH) comments in response to the Office of the State Comptroller's (OSC) Draft Audit Report 2001-S-43 entitled "Health Care Initiatives Pool Disbursements" (HCIPD).

Our response to the specific recommendations is as follows:

Recommendation #1:

Establish and enforce compliance with formal policies and procedures for verifying the legitimacy and accuracy of HCI pool disbursements. At a minimum, the Department should:

(a) Require that disbursements contain sufficient documentation to support the expense.
(c) Obtain and document the necessary Department approvals for disbursements.

Response:

Department staff which have been assigned to administer each project contract are responsible for reviewing documentation and approving contract payments to the contractor. Such contracts are subject to procedures which mirror State Finance Law processes for contracts funded through State appropriations. In recommending payments under these contracts, the Department contract administrator must provide the Division of Health Care Financing (DHCF) with a memorandum authorizing contract payments. As OSC knows, the Department has a very comprehensive internal approval process for disbursements from the HCIPD fund. That process requires a total of six individuals to review and approve the package supplied by the contract administrator prior to processing payments. Upon completion, the DHCF's Assistant Director signs the authorization letter directing the Pool Administrator to issue a check for payment of each contract voucher. The DHCF Assistant Director will not sign the payment authorization letter without proof that the voucher package has gone through the procedures described above. This proof is in the form of an internal buckslip with sign-off blocks for individuals involved in the above referenced review and approval process. The Division will retain all related buckslips as proof that vouchers have been reviewed and approved prior to payment.

Response (cont'd):

(b) Improve the controls over formulaic HCI Pool disbursements to minimize the risk that payments will be made to providers who are not entitled to funding.

Response:

As stated in the audit findings, only one formulaic funded provider inappropriately received funds for Pool Year 2000. The Department recovered monies paid to such provider and redistributed such funds to remaining eligible providers in May 2002. There were no errors in the calculation or distribution of 1999 Diagnostic and Treatment Center (D&TC) pool funds. This error occurred as a result of the Department's initiative to ensure adequate cash flow to the D&TC provider community. At the time, delays in the calculation of the initial distributions model prevented Year 2000 distributions from being made timely. The prior year's model was used on an interim basis until the 2000 model was completed. In doing so, the list of providers to receive these interim payments were those providers eligible in 1999. The 2000 listing was not available at the time.

The Department's record of ensuring that only eligible providers receive formulaic based disbursements is outstanding. To further strengthen that record, we've implemented additional procedures.

(d) Improve the reconciliation process to detect errors in payment information, missing authorizations and potential duplicate payments.

Response:

Payments are only issued based on written notification from the Department. In the one case cited, verbal approval was given to issue a second check after assurances were received from the Pool Administrator that a stop payment was issued on the first check. Follow-up email documentation was inadvertently omitted in this instance. As a general rule, directives from the Department to the Pool Administrator to reissue checks subsequent to a stop payment are transmitted either by email, fax, or in writing. Stop payments and check reissues are footnotec in the monthly reports submitted by the Pool Administrator to the Department.

The Pool Administrator and the Department will continue to monitor issues concerning outstanding checks and stop payments. Further, the Department will periodically review and reinforce with staff the need for written documentation of directives to the Pool Administrator.

The discrepancies in payment information noted in the report occurred when there was an inconsistency in the payment package between the address shown on the authorization letter and that on the transmittal page. In such cases, the Department has instructed the Pool Administrator to use the information on the transmittal page.

Response (cont'd)

Another situation, where three addresses were not recorded, occurred in 1999. The Pool Administrator modified their computer system in late 1999 so that this situation would no longer occur. Is should be noted however, that in all cited cases, disbursements were made to the correct providers.

To strengthen procedures in these areas, the Pool Administrator will notify the Department of changes in the payment packages and request clarification of these types of issues prior to making disbursements. Verification of appropriate action will then be transmitted back to the Pool Administrator, ensuring proper disbursement.

Recommendation #2:

Make sure each contract is fully approved before its intended start date.

Response #2:

It is not uncommon for contractors to voluntarily commence activities under the contract prior to final execution and approval. In all such cases, the Department advises such contractors that they are proceeding at their own risk in the event the contract is not ultimately approved. It is the Department's position that a contract start date that predates the contract's final approval and execution is not prohibited by any applicable provisions of the State Finance Law or otherwise. It is often advantageous to the State, to the contractors, and to the populations to be served pursuant to the contracts, to maximize the flexibility to pay for services performed before final approval of the contracts by providing for start dates before approval dates.

Recommendation #3:

Require Excellus to improve controls over its automated system by:

(a) Strengthening logical security by optimizing logical security settings and features; renaming the Administrator Account; posting a legal notice about the system's proprietary nature at log-in; and properly documenting all system changes.

Response #3:

The Department will update policies and procedures requiring Excellus to incorporate these recommendations.

(b) Enhancing physical security by using electronic key cards and logging access to the server room; disabling floppy drives at workstations; and clearing sensitive data and software from equipment before retiring it.

Response:

The Excellus offices are only accessible by a key card security system, which limits physical access to employees or supervised visitors. Access to the computer room has been limited to essential personnel and management. In addition, Excellus has:

- upgraded the security system on March 11, 2002, initiating key card access to the computer room by designated staff only and maintaining electronic access logs;
- disabled floppy drives for any workstations where staff does not require such access for related work duties;
- assigned responsibility for clearing information from hard drives, when necessary, to a system administrator; and
- instituted procedures for reviewing with the Department, any standard forms or documentation necessary to ensure that all discarded or transferred equipment is examined and cleared of all sensitive information prior to release.

(c) Upgrading its Business Continuity/Disaster Recovery Plan, including fully documenting and annually testing its plan's effectiveness through disaster and recovery simulation exercises; identifying a sufficiently remote alternative disaster recovery site; installing adequate environmental controls; and keeping a current version of Excellus' operating system at the remote site.

Response:

Excellus provided the OSC with its Disaster Recovery Plan, which contained plans for an alternate disaster recovery site. The Department and Excellus are reviewing and updating the Plan to include an alternate Disaster Recovery site should the Blue Cross building not be accessible. Once finalized, the Department and Excellus will perform annual tests of the system which will include a test of the alternate recovery site. As part of the Disaster Recovery Plan, Excellus will create and maintain duplicates of the operating system in their most current versions and store them at an off site location.

The Department and Excellus will consult on and implement the necessary environmental control protection systems for the Excellus computer hardware.