

ALAN G. HEVESI  
COMPTROLLER



110 STATE STREET  
ALBANY, NEW YORK 12236

STATE OF NEW YORK  
OFFICE OF THE STATE COMPTROLLER

November 4, 2004

Vincent A. DeIorio, Esq.  
Chairman  
New York State Energy Research and Development Authority  
17 Columbia Circle  
Albany, NY 12203-6399

Re: Internal Controls Over Financial Operations  
Report 2004-S-55

Dear Mr. DeIorio:

Pursuant to Article X, Section 5 of the State Constitution and Section 2803 of the Public Authorities Law, we have audited the New York State Energy Research and Development Authority's system of internal controls over its financial operations for the period April 1, 2002 through March 31, 2004.

**A. Background**

The New York State Energy Research and Development Authority (Authority) was established in 1975 by Article 8, Title 9 of the Public Authorities Law, and is involved in a number of energy-related activities. The Authority funds research to develop new energy technologies and expand the use of the State's indigenous and renewable energy resources, while reducing adverse environmental effects associated with energy production in use. The Authority administers the New York Energy Smart<sup>SM</sup> program, which is funded by a system benefit charge on the electricity transmitted and distributed by the State's investor-owned utilities. The Energy Smart<sup>SM</sup> program provides energy efficiency services for low-income and other populations, research and development, and environmental protection activities. The Authority also provides financial and technical assistance to customers seeking to assess and implement cost-saving energy efficiency measures. The Authority also monitors energy supply, consumption and emissions in the State, and periodically reports the results of its monitoring to government officials and the public.

The Authority manages, on behalf of the State, the Western New York Nuclear Service Center at West Valley, Cattaraugus County, where the U.S. Department of Energy, through a contractor, is cleaning up high-level nuclear wastes. The State's low-level radioactive waste storage facility is also located at that site, and the Authority maintains and monitors this facility.

The Authority owns, on behalf of the State, a 280-acre parcel of land in Saratoga County, which is used as a business park devoted to the development of new, clean energy technologies. It

also issues bonds and notes that provide tax-exempt financing for certain energy-related projects. The bonds and notes may be issued to electric and gas utilities and other private entities. The Authority derives its basic research revenues from an assessment on the intrastate sales of New York State's investor-owned electric and gas utilities, and voluntary annual contributions by the New York Power Authority and the Long Island Power Authority. Additional research dollars come from limited corporate contributions. The Authority can obtain Federal funding to identify existing technologies and equipment that can reduce the energy costs of its customers. The Authority is managed by a President, who reports to a 13-member Board of Directors (Board). The Board meets quarterly. The Authority has 204 employees with an annual payroll of about \$13 million. For the year ended March 31, 2003, the Authority had revenues of about \$205.6 million and expenses of about \$190 million.

## **B. Audit Scope, Objectives and Methodology**

Pursuant to the New York State Governmental Accountability, Audit and Internal Control Act of 1987 (Act), as revised in 1999, the Authority's management is responsible for establishing and maintaining an effective system of internal controls and a program of internal control review. In addition, in accordance with the New York State Division of the Budget's Policy and Reporting Manual Item B-350, State agencies and public authorities must annually certify their compliance with important provisions of the Internal Control Act, and submit this certification of compliance to the Division of the Budget. We audited the Authority's system of internal controls over its financial operations for the period April 1, 2002 through March 31, 2004. The objectives of our performance audit were to assess the adequacy of the Authority's system of internal controls over its financial operations and to express an opinion on this system based upon our audit.

To accomplish these objectives, we interviewed Authority officials and reviewed policies and procedures governing the following significant financial operations: Board oversight and governance, revenue and collections, cash and investments, payroll, procurement and contracting, equipment and asset management, budgeting and expenditure control, and accounting and information systems. We interviewed Authority staff responsible for these financial operations and performed limited compliance testing to provide assurance that Authority employees follow established policies and procedures.

During the 2002-03 fiscal year, the Authority reported it had 3,273 contract actions which led to the commitment of \$267 million. Contract actions include new contracts, contract modifications, and individual task (work) orders issued. Only 92 contract actions, which committed \$13.3 million during the period related to goods and services. The remaining 3,181 contract actions, which committed \$253.6 million, relate to research and development grants or provided incentives for conversion to more efficient energy systems. We plan to return and examine program contracts as part of a separate audit.

We conducted our audit in accordance with Generally Accepted Government Auditing Standards. Such standards require that we plan and do our audit to adequately assess those procedures and operations included within the audit scope. Further, these standards require that we understand the Authority's internal control systems and compliance with those laws, rules and regulations that are relevant to the Authority's procedures and operations that are 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.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State, several of which are performed by the Division of State Services. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under Generally Accepted Government Auditing Standards. In our opinion, these management functions do not affect our ability to conduct independent audits of program performance.

### **C. Results of Audit**

In our opinion, management's certification referred to above is fairly stated in all material respects based on the criteria set forth in the Act and Item B-350. However, we noted the following instances in which the Authority could either improve its system of internal controls, or strengthen the adherence to existing policies and procedures. Authority officials indicated that they are currently reviewing their overall operations and will seek to formalize, establish, improve or update policies and procedures over several areas. They further indicated that they have already implemented some of the recommendations in this report. Additional information about these matters and about other aspects of the Authority's internal controls, including areas in which the controls are strong, is contained in Table I at the end of this report.

1. According to Section 2879(3)(b)(ii) of the Public Authorities Law, any contract requiring services rendered for a period of more than one year must be approved by the governing board of that Authority. The Authority Board technically approves all service contracts in excess of one year by an annual ratification as required by Law. However, we found that while the Authority meets the minimum standards in this regard, some improvements are needed to bring it into full compliance with the purpose of the statute. The Board approval is based mainly on annual ratification after the contracts are executed by management, but pre-approval should occur where feasible and ratification should be the exception rather than the rule. Additionally, contracts or lists of contracts should be presented at each quarterly Board meeting so that contracts are approved or ratified as near to the execution date as possible. Under the current process, contracts may be in effect for nearly a year prior to being ratified by the Board. Another weakness noted is that the Board resolution to approve the contracts refers to the annual procurement contracts report which is actually designed to satisfy a separate requirement of the Public Authorities Law. The resolution approving service contracts in effect longer than one year should refer specifically to those contracts rather than an annual contract report to better separate the two requirements.

2. When we reviewed selected billings and past due accounts, we identified a number of late billings and one inaccurate billing. We reviewed six Authority bills totaling about \$46,000 for certain third-party reimbursement contracts. This type of contract generated \$1.47 million in revenue for the year ended March 31, 2003, about 8 percent of the Authority's third-party revenue and less than 1 percent of its total program revenue for that year. In this type of contract, the Authority hires a consultant to perform a study for a third party; the Authority pays the consultant and is reimbursed by the third party. For the six transactions we tested, the third-party customer was to send in payment six months after receiving either the consultant's report or the award letter from the Authority. However, four of the six bills (totaling about \$32,100) were sent late by the Authority. One bill (about \$9,700) was two years late, and three bills (about \$22,400) were six to nine months late. In addition, one of the bills was not accurate, as it totaled \$9,630 when it should have totaled \$9,682. We also reviewed five past due accounts, which totaled about \$82,000, and found that for three of these bills (\$29,962) were issued more than a year late, one bill (about \$38,500) was issued more than nine months late, and one bill (about \$13,500) was issued more than three months late.

Authority officials stated that the six billings we reviewed are not representative of all their billings for third-party reimbursement contracts, because different billing procedures are used for other third-party contracts. They further stated that the bills were late because they were issued when payments were made to the contractors, rather than when the consultant reports/award letters were sent to the customers. During our review, the Authority completed changes to its information systems which should provide better monitoring of when bills should be sent.

3. We found that past due accounts were not pursued in a timely manner. According to the Authority's procedures, the customer is to be sent a second invoice between 66 and 96 days after the initial invoice. The customer is to be contacted for payment a third time between 97 and 127 days after the initial invoice. If an account is still not paid 120 days after the initial invoice, the Authority may refer the account for collection. We tested the Authority's compliance with these procedures for five past due accounts totaling about \$82,000. We found that, for one of these accounts (totaling \$13,500), the second invoice was sent to the customer 16 days late, and for three of the accounts (totaling about \$40,500), the third invoice was sent to the customer between 13 and 270 days late. Four of the five accounts were eventually paid, the payments being made between 178 and 613 days after the initial invoices were sent. The fifth account (totaling about \$7,600) has not been collected, and was not turned over to the State Attorney General's Office for collection until 581 days after the initial invoice was sent.
4. We made recommendations for improving the Authority's controls over cash. First, the Authority's policies and procedures do not require the maintenance of a daily log of cash receipts. In the absence of such a log, the Authority has no assurance all cash receipts are deposited and recorded. The Authority should maintain such a log and periodically reconcile the log to both the bank deposits and the accounting records. The Authority also needs to separate the following cash-handling duties among more than one employee: maintaining custody of the checks, preparing deposit slips, and posting the receipt of checks to the accounting records. The Authority does not restrictively endorse checks before they are

deposited. Rather, the checks are deposited by a State agency, and the agency does not allow the Authority to endorse the checks. During our audit, the Authority began using a cash receipts log. Subsequent to our audit, the other State agency provided the Authority with an endorsement stamp.

5. We recommended improvements to the Authority's controls over procurement and contracting. First, duties are not adequately separated among different employees, because the person who places orders also confirms that the goods were received. Second, a partial payment on a contract was not supported by documentation of the related labor and material costs, as required by the contract. Such payments should not be made unless the payment requests are supported by appropriate documentation.
6. To safeguard its equipment, the Authority should restrict personal use of such equipment and monitor its use. We found that the Authority blocks access to certain internet sites, but does not monitor employee internet usage to determine if it is appropriate. Also, employees do not need prior approval to install software on their computers (including software downloaded from the internet) and to delete installed software from their computers. This increases the likelihood that Authority equipment could be used for personal purposes and computer viruses could be admitted into the Authority's computers. We also found that a vehicle usage log was not up-to-date.
7. To prevent unauthorized access to critical computer systems, the Authority should restrict employee access to the systems necessary for their duties and require a strong system of password protection. We found that some Accounting and Finance Unit staff have user access to the Human Resources module. Generally, employees outside the Human Resources office should either have no access, or read-only access, to the data in this module. Accounting and Finance staff also have unrestricted access to all accounting system modules to which they have been assigned. However, their access should be restricted to their primary areas of responsibility. We also identified employee passwords that are not complex and are not required to be changed periodically. We further determined that the Authority lacks a formal disaster recovery plan to provide for continued data processing in the event of data loss or other disaster. Subsequent to our audit, the Authority implemented a password policy that requires complex passwords which are changed quarterly. Authority officials also told us that they intend to restrict employee access to the functions within each module needed to do their job.

### **Recommendations**

1. *Revise current procedures for obtaining Board approval of service contracts exceeding one year in duration, by providing for pre-approval of contracts whenever feasible, presenting contracts for approval quarterly rather than annually, and reference the document listing specific contracts being presented for approval in the Board resolution.*
2. *Improve the timeliness of third-party billing and collection practices.*
3. *Improve cash receipts controls by logging cash receipts daily upon receipt, restrictively endorsing checks, periodically reconciling the cash log to bank deposits and the accounting*

*records, and separating check custody from other cash receipts duties such as preparation of deposits and posting of receipts to the accounting records.*

4. *Improve controls over purchasing by separating duties for authorizing payment for goods from the ordering department, and verifying that progress payments on contracts are properly supported.*
5. *This recommendation was deleted based on information provided in the Authority's reply.*
6. *Improve computer system access controls by restricting employee access to only the functions they need, utilizing more complex passwords that are changed more frequently, and formalizing and periodically testing a disaster recovery plan.*

A draft copy of this report was provided to New York State Energy Research and Development Authority officials for their review and comment. With the exception of recommendation number 5, Authority officials agree with our recommendations and noted efforts that they have taken to implement them. Their comments have been considered in preparing this final report, and are included as Appendix A.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the President of the New York State Energy Research and Development Authority shall report to the Governor, the State Comptroller, and the leaders of the Legislature and its 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 Gerald Tysiak, Stephen Goss, Wayne Bolton, Kathleen Hotaling, Sharon Salembier and Dana Newhouse.

We wish to thank the management and staff of the New York State Energy Research and Development Authority for the courtesies and cooperation extended to our auditors during this audit.

Very truly yours,



Carmen Maldonado  
Audit Director

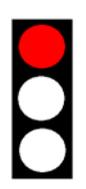
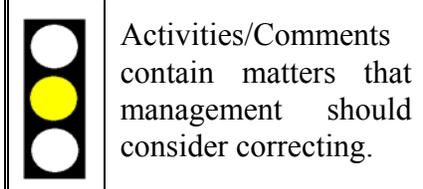
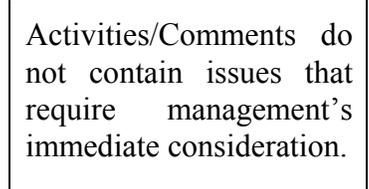
cc: Robert Barnes, Division of the Budget

**TABLE I**

**NEW YORK STATE ENERGY RESEARCH AND DEVELOPMENT AUTHORITY  
INTERNAL CONTROLS OVER FINANCIAL OPERATIONS**

A colored “traffic light” legend is included in the table below to assist management in focusing an appropriate level of attention on the issues summarized in the table. As part of our audit, we sought answers to a series of questions and reviewed selected Authority records related to certain financial operations. Our questions in each area, along with a summary of the Authority’s activities and our comments concerning these activities, are included in the table.

**Legend:**

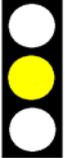
	Activities/Comments contain matters that should be of immediate concern to management.		Activities/Comments contain matters that management should consider correcting.	 Activities/Comments do not contain issues that require management’s immediate consideration.
---	--	--	---	--

	QUESTION	AUTHORITY ACTIVITIES	COMPTROLLER’S COMMENTS
<b>A. Board Oversight and Governance:</b>			
	Does the Authority’s Board of Directors function in a manner that promotes an ethical business climate within the organization and encourages and supports full compliance with all applicable laws, rules and regulations?	The Authority has adopted Conflict of Interest Requirements that generally follow the provisions of the Public Officers Law and which officers and staff must follow. The Conflict of Interest Requirements constitute the Authority’s Code of Ethics. The Board is subject to the Public Officers Law. There is some guidance in the Personnel Handbook and the Procurement Guidelines related to independence and contracting. The Board also reviews, approves, and submits to State oversight entities all reports required by law.	The Authority process for obtaining Board approval for contracts for services in excess of one year meets the technical minimum requirements of the law. However, improvements are needed to bring the Board’s approval process into full compliance with the intent and spirit of the law.  See “Results of Audit issue # 1”
	Has the Authority’s Board of Directors established appropriate controls that promote the economic,	The Authority routinely reviews and updates policy and procedures manuals and distributes them to staff. The Authority’s contract award	Our audit indicated that the Board has established controls that promote economic, efficient and effective operation that provide transparency and accountability of

**TABLE I (Cont'd)**

	<b>QUESTION</b>	<b>AUTHORITY ACTIVITIES</b>	<b>COMPTROLLER'S COMMENTS</b>
	<p>efficient and effective operation of the Authority consistent with its statutory public benefit mission and that provide for transparency and accountability in pursuing its strategic business objectives?</p>	<p>process includes the use of outside reviewers in evaluating solicitations. The Authority also provides State oversight entities with all required reports.</p>	<p>objectives. In addition, we noted that one Board member's term expired in March 2000. Because the member still serves, there are no Board vacancies. However, one Board member did not attend any Board meetings during the period September 2002 through September 2003.</p>
<p><b>B. Revenue and Collections:</b></p>			
	<p>Do the Authority's policies and procedures provide assurance that revenues are billed timely and accurately and are recorded properly in the accounting records?</p>	<p>The Authority has five major sources of revenue: draw downs of State appropriations, Federal grants, two contractual schedule payments, and reimbursement contracts with third parties. Contractual schedule payments are received automatically and the Authority only bills if payment is not received on the scheduled date. Payments on contracts with third parties are due when specific benchmarks in the project are reached; however, the Authority generally bills the third-party to remind them of their obligation.</p>	<p>Our testing identified instances in which the Authority's billings were late or inaccurate. The Authority should implement procedures to improve the timeliness and accuracy of its billings. (Authority officials contend that because the contract states when reimbursement to the Authority is due, they are not required to send a bill to the customer. Sound internal controls require that bills be sent when payment is due, even when the payment benchmark is specified in the contract.)</p> <p>We limited our testing of billings to third-party reimbursement contracts, which are the largest revenue source billed by the Authority and account for about 8 percent of third party revenue and less than one percent of total program revenue.</p> <p>See "Results of Audit issue # 2"</p>
	<p>Do the Authority's policies and procedures provide assurance that revenues are being collected timely?</p>	<p>The Authority has established policies and procedures for identifying and collecting on past due accounts.</p>	<p>Our test of past due accounts found that invoices were sent out late and the amounts due were not promptly collected. The Authority should take steps to improve the timeliness of its collections. Authority officials told us they completed changes that will enable them to better monitor invoicing dates.</p> <p>We limited our testing of revenue collection to third-party reimbursement contracts, which are the largest revenue source billed by the Authority and account for about 8 percent of third party revenue and</p>

**TABLE I (Cont'd)**

	<b>QUESTION</b>	<b>AUTHORITY ACTIVITIES</b>	<b>COMPTROLLER'S COMMENTS</b>
			less than one percent of the total program revenue.  See "Results of Audit issue # 3"
<b>C. Cash and Investments:</b>			
	Do the Authority's policies and procedures provide assurance that cash and investments are properly safeguarded, accounted for, and deposited into the appropriate accounts?	The Authority has five bank accounts that are managed by the New York State Department of Taxation and Finance (Tax & Finance). Authority staff receive payments, record the receipt in the proper accounts, and prepare bank deposits. Tax & Finance endorses the checks and makes the bank deposits. Tax & Finance also maintains canceled checks and provides a list of outstanding checks to the Authority. The Authority reconciles their accounts to bank statements.  Investment policies are reviewed and approved annually by the Board. The Authority authorizes the purchase and sale of investments, which are maintained by Tax & Finance.	To improve internal controls over cash, the Authority should use a cash receipt log to independently record cash receipts and should restrictively endorse checks when they are received. The Authority should also separate duties so that a single employee does not have custody of the checks, prepare deposit slips, and post the receipt of the checks to the accounting records.  See "Results of Audit issue # 4"  Our audit indicated that the Authority's investment policies and procedures are being followed.
	Do the Authority's policies and procedures provide assurance that cash disbursements are properly authorized and recorded?	Each week the Authority prepares a report of outstanding invoices, the warrant for payment, and the payment checks. Payments are made by the appropriate due date and before interest charges are due. Warrants and checks are reviewed by the Controller before they are sent to Tax & Finance, where the checks are signed.	Our audit indicated that the Authority's policies and procedures are being followed.

**TABLE I (Cont'd)**

	<b>QUESTION</b>	<b>AUTHORITY ACTIVITIES</b>	<b>COMPTROLLER'S COMMENTS</b>
<b>D. Payroll:</b>			
	Do the Authority's policies and procedures provide assurance that employee time and attendance records are accurate and that leave time is accounted for and recorded properly?	The Authority uses an automated software package for employee time and attendance records. Employees and supervisors sign electronic time sheets using system features; leave accruals are automatically recorded by the system. The Finance Unit verifies that timesheets are completed properly and accruals and overtime are reasonable.	Our audit indicated that the Authority's policies and procedures are being followed.
	Do the Authority's policies and procedures provide assurance that payroll changes (e.g., additions, deletions, and overtime) are processed accurately and timely?	Appointment letters for new employees are approved by either the President or Vice President for Administration and payroll additions are entered into the computer system by Human Resources. Finance is notified of all personnel changes each pay period and verifies that the payroll changes are documented. Prior approval is required for overtime.	Our tests of payroll transactions showed that the Authority's procedures were followed. We did not test overtime transactions because total overtime paid was less than one percent of total payroll costs.
<b>E. Procurement and Contracting:</b>			
	Do the Authority's policies and procedures provide assurance that purchases are authorized, received, and recorded properly?	The Board has adopted policies and procedures that require authorization for all purchases at all purchase levels. Contracts and purchase orders are executed by the Treasurer. Mailroom staff receive and sign for deliveries. However, the ordering department is responsible for counting and inspecting the goods received and approving payment for the order. Finance Unit staff process the payments.	To improve internal controls over purchases of goods, the Authority should implement procedures to independently verify that goods ordered have been received. The Authority should also verify that progress payments on contracts are supported as required by the contracts.  See "Results of Audit issue # 5"
	Do the Authority's policies and procedures provide assurance that purchases are reasonable and necessary and made in an economical and efficient manner?	The Authority has established dollar-level thresholds for requiring bids and for buying goods and services off State contract.	Our tests showed that Authority procedures were followed.

**TABLE I (Cont'd)**

	<b>QUESTION</b>	<b>AUTHORITY ACTIVITIES</b>	<b>COMPTROLLER'S COMMENTS</b>
<b>F. Equipment and Asset Management:</b>			
	Do the Authority's policies and procedures provide assurance that equipment acquisitions and dispositions are authorized and recorded properly, and that a comprehensive inventory of equipment is maintained?	The Authority maintains equipment inventory records and conducts a complete physical inventory every two years.	Our tests showed that Authority procedures were followed. With the exception of one acquisition, which lacked documentation showing that it was authorized, all acquisitions were properly documented.
	Do the Authority's policies and procedures provide assurance that equipment is secured properly and used as intended?	The Authority has policies prohibiting the personal use of equipment, and maintains usage logs for three of its five vehicles. The Authority also blocks access to various internet sites.	To improve internal controls over equipment security and use, the Authority should monitor vehicle logs to ensure usage is documented and appropriate, monitor internet use, and require employees to obtain prior approval before installing software onto their computers and deleting software from their computers. See "Results of Audit issue # 6"
<b>G. Budgeting and Expenditure Control:</b>			
	Do the Authority's policies and procedures provide assurance that its annual budget is prepared accurately and timely?	Each year the Treasurer and the Controller/Assistant Treasurer prepare budget worksheets containing budgeted expenditures for the current year, expenditures for the prior year and a column for the requested amount by program. The worksheets are sent to Program Directors and Managers for review along with staff and salary information. The Managers and Directors complete and return the worksheets. The worksheets are reviewed, and the data is entered in the accounting system and "rolled-up" to aggregate the data. The aggregate data is presented to the President and used as the basis for the budget request package. The budget is reviewed and approved by the Board.	Our audit indicated that the Authority's annual budget is prepared timely and with consideration of prior years' actual results and expectations for the year in question.
	Do the Authority's policies	The Authority uses a Budget	Our audit indicated that the

**TABLE I (Cont'd)**

	<b>QUESTION</b>	<b>AUTHORITY ACTIVITIES</b>	<b>COMPTROLLER'S COMMENTS</b>
	<p>and procedures provide assurance that actual operating results are monitored against budgeted estimates and that appropriate revisions to current and future budgets are made as warranted by these operating results?</p>	<p>Status Report that compares budgeted and actual amounts to monitor budget performance.</p>	<p>Authority is following its policies and procedures.</p>
<p><b>H. Accounting and Information Systems:</b></p>			
	<p>Do the Authority's accounting and information systems provide assurance that management has access to timely, accurate and relevant information?</p>	<p>The Authority uses software packages for its various accounting, time and attendance, and project management functions. These systems enable the Authority to have timely, accurate and relevant accounting information.</p>	<p>Our audit indicated that the Authority is following its policies and procedures.</p>
	<p>Do the Authority's policies and procedures provide assurance that the accounting and information systems are secure and that the information is recoverable in case of system failure?</p>	<p>The Authority provides employees with user access to the software modules related to the unit they are assigned to. The various software packages also require passwords. The Authority performs daily back-up of network data including proper storage of the back-up data. The Authority has a firewall and monitors logs from the firewall.</p>	<p>To improve internal controls over accounting and information systems, the Authority should restrict employees' user access to the software modules they need to do their jobs, providing read-only access if employees need only to view data. The Authority should also require that passwords be changed frequently and be complex, and should implement and test a formal disaster recovery plan.</p> <p>See "Results of Audit issue # 7"</p>



**New York State Energy Research and Development Authority**

Vincent A. Delorio, Esq., *Chairman*  
Toll Free: 1 (866) NYSERDA  
www.nysesda.org • info@nysesda.org

September 20, 2004

Carmen Maldonado  
Audit Director  
State of New York  
Office of the State Comptroller  
110 State Street  
Albany, New York 12236

Dear Ms. Maldonado:

This letter is in reply to your draft audit report (2004-S-55) on the New York State Energy Research and Development Authority's system of internal controls over its financial operations for the period April 1, 2002 through March 31, 2004. We are pleased with the unqualified opinion rendered in your report regarding our internal control certification, which reflects well on the effective system of internal controls created and implemented by the Authority's staff and management, under the direction of its Board. In addition, the draft audit report contains recommendations for further strengthening the Authority's system of internal controls, each of which we address below.

1. *Revise current procedures for obtaining Board approval of service contracts exceeding one year in duration, by providing for pre-approval of contracts whenever feasible, presenting contracts for approval rather than annually, and reference the document listing specific contracts being presented for approval in the Board resolution.*

**Response:** As you know, NYSERDA presents a semi-annual listing of its contracts to the Board, usually at the January meeting, and an Annual Procurement Contracts Report containing a listing of its existing contracts to the Board for approval, at the June meeting. NYSERDA concurs with the Comptroller that providing the Members with a listing of contracts entered into, or expected to be entered into, for approval at each meeting will result in contracts being approved or ratified as near to the execution date as possible. It also provides the Members with more up-to-date information on contracting activities as well as additional information on the status of Authority programs and costs incurred. NYSERDA will therefore amend its procedures to provide information on contract actions at each of its

---

**Main Office**  
Albany  
17 Columbia Circle  
Albany, NY 12203-6399  
Toll Free: 1 (866) NYSERDA  
Phone: (518) 862-1090  
Fax: (518) 862-1091

**West Valley Site**  
Management Program  
10282 Rock Springs Road  
West Valley, NY 14171-9799  
Phone: (716) 942-4387  
Fax: (716) 942-2148

**New York City**  
485 Seventh Ave., Suite 1006  
New York, NY 10018  
Phone: (212) 971-5342  
Fax: (212) 971-5349

**Buffalo**  
617 Main Street, Suite 105  
Buffalo, NY 14203  
Phone: (716) 842-1522  
Fax: (716) 842-0156

regularly scheduled meetings. The information will include a list of contract executed since the last meeting as well as as contracts expected to be executed.

Although NYSERDA Members provide the annual approval required for contracts exceeding one year as required by the Public Authorities Law, we will, as suggested by the Comptroller, make reference to such contracts in that resolution.

2. *Improve the timeliness of third-party billing and collection practices.*

**Response:** As noted in the Comptroller's report, NYSERDA initiated changes to its computerized systems prior to the Comptroller's review to improve the ability to monitor the dates upon which certain third-party billings may be billed in instances where reimbursement is due upon a conditional event, such as receipt of a technical report or receipt of an incentive award letter from NYSERDA.

Regarding collection procedures, NYSERDA has reinforced to staff the importance of complying with NYSERDA's policies, in order to provide for more timely and regular collection efforts for outstanding receivables.

3. *Improve cash receipts controls by logging cash receipts daily upon receipt, restrictively endorsing checks, periodically reconciling the cash log to bank deposits and the accounting records and separating check custody from other cash receipts duties such as preparation of deposits and posting of receipts to the accounting records.*

**Response:** As noted in the Comptroller's report, the Authority implemented, during the audit, the Comptroller's recommendation to institute a log to record receipts of checks which are independently reconciled to bank deposits and the accounting records.

The Comptroller's recommendation to segregate check custody functions relates to the fact that the Accounting staff person who is responsible for preparation of deposit slips and posting of receipts into the accounting records also has physical custody of the checks for a brief period of time to make photocopies of these materials. To improve our system of controls, this responsibility has been reassigned to another individual in the Accounting unit, who has no involvement in preparing or recording the deposits.

4. *Improve controls over purchasing by separating duties for authorizing payment for goods from the ordering department, and verifying that progress payments on contracts are properly supported.*

**Response:** The Comptroller's report notes that for certain administrative purchases, the Authority's prior policies and practices did not require an approval for receipt of the goods independent of the individual approving the vendor's invoice, which might also be the individual responsible for ordering the goods. The Authority's

policies have been changed to require the written approval of an individual independent of the individual approving the vendor invoice for payment to provide for proper segregation of duties over purchasing and receiving authorizations.

Regarding verification that vendor invoices are properly supported with appropriate backup documentation consistent with contractual requirements, policies have been developed to require the review of appropriate supporting documentation by the Finance department in order to process vendor invoices for payment; invoices not properly supported will be returned to the vendor.

5. *Improve equipment controls by monitoring employee usage of the internet, restricting employees' ability to add and delete software from computers and monitoring vehicle logs to determine if they are up to date.*

**Response:** Employee usage of the Internet must be Authority-related and this is set forth in the Authority's internal control manuals. In addition, NYSERDA uses a *preventative* control procedure through a third-party, industry-accepted Internet blocking software package (Websense) to restrict employee's access to Internet sites which clearly do not have a business purpose, including industry-labeled topical areas which have no clear business purpose. In fact, Comptroller's staff tested the functioning of this software by attempting to access several sites which were not business-related, and confirmed that the blocking software prevented access. NYSERDA supervisors are also responsible for initiating disciplinary procedures for employees observed accessing non-business-related sites.

We feel that the control procedures being used are the most effective manner for controlling the risk of unauthorized Internet usage and provide the Authority with reasonable assurance that usage is appropriate.

Regarding the recommendation to restrict employee's ability to add or delete programs, we feel that our current procedures provide an effective way to accomplish these control objectives. The Authority's policy manuals clearly state that employees may not load programs onto their personal computer or the network server without prior approval of the Computer Services unit. However, the operating system does not restrict an employee from doing this. All computers have anti-virus software installed on them, which performs a full virus scan on a daily basis. A virus shield also runs continuously to detect and block virus-like activity. In addition, the Computer Services unit periodically reviews the files and programs loaded on each employee's computer and if programs are present which were not approved, appropriate disciplinary procedures may be initiated. We feel these control procedures provide a cost-effective way to reduce the risk of unauthorized computer program access and vulnerability.

The Comptroller's review of Authority vehicle usage logs noted that one day there

was approximately 50 miles of usage which was undocumented. Employee use of Authority-owned vehicles is restricted to business use by written policy. Employees may only use Authority-owned vehicles with pre-approval by the Facility Manager and his/her staff, which includes providing an indication of the destination and duration of the usage. The vehicle logs used by the Authority are meant to provide a usage history in the event that problems occur, as well as to document overall vehicle usage. Using this procedure, we were able to provide the information necessary to update the log. Staff believes existing procedures are adequate.

6. *Improve computer system access controls by restricting employee access to only functions they need, utilizing more complex passwords that are changed more frequently, and formalizing and periodically testing a disaster recovery plan.*

**Response:** NYSERDA implemented the Comptroller's recommendations regarding access rights to the accounting software: certain accounting staff who had access to the human resources module were provided read-only access; and access to functions within each accounting module were granted only where an employee had a clear need for access to such functions.

The Authority implemented a new password policy, consistent with standards required by the New York State Office of Cyber Security & Critical Infrastructure Coordination, which provides for standards for password construction and change frequency.

Regarding the recommendation for development of a disaster recovery plan, a multi-disciplinary working group has been formed and is in the process of developing this plan.

We also communicated to your staff several suggested editorial changes and pointed out certain other references that should be changed in the final report. The editorial changes include substituting "recommendations" for the references to "weaknesses" and "deficiencies" in order to be consistent with language used elsewhere in the report, as well as to be consistent with the report's overall conclusion. The other changes included: (1) eliminating or substantially altering the statement on page 2 that "the Authority's procurement system cannot identify new contracts entered into during the period", since the system is performing this function, and the Comptroller's staff was advised of this; (2) eliminating or changing the statement on page 2 which states "we did not review the latter category of contracting actions", since some contracting actions were reviewed; and (3) revising the sentence on page 8 to make clear that the third-party reimbursement contracts tested by the Comptroller's Office account for about 8 percent of the Authority's third-party revenue, but only less than 1 percent of its *total* program revenue. Our discussions with your staff indicated that you may revise your final audit report to address these issues.

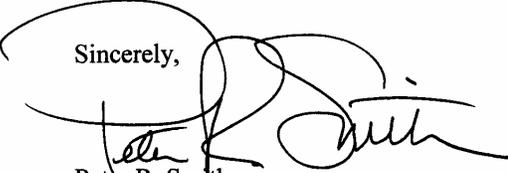
\*  
Note

We appreciate the recommendations contained in your report to help improve the Authority's system of internal controls. We also thank you and your staff for the professionalism displayed during the course of your examination.

\*Note: We revised the audit report to address the Authority's editorial changes.

Please contact me if you have any questions or need additional information.

Sincerely,

  
Peter R. Smith  
President