ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

May 30, 2003

Mr. Pierre Alric
Acting President
New York State Higher Education Services Corporation
99 Washington Avenue
Albany, New York 12255

Re: TAP Application Process
Report 2002-S-41

Dear Mr. Alric:

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 selected general and application controls over the Tuition Assistance Program (TAP) for the period of April 1, 2001 through December 31, 2002.

A. Background

The Higher Education Services Corporation (HESC) was established in 1974 to provide centralized processing for student financial aid programs for post-secondary education. HESC administers New York State's Tuition Assistance Program (TAP), the Federal Family Education Loan Program, and other State and Federal aid programs.

TAP annually provides eligible undergraduate and graduate students with need-based grants worth as much as $5,000 each to help them meet tuition charges. During the 2001-02 fiscal year, HESC paid $675 million in TAP grants to more than 350,000 students. Eligibility for TAP and the amount of each award are based on several factors, including residency and income.

To enhance the administration of financial aid through automation, HESC has established the Electronic Financial Aid Network (EFAN). The network consists of various computer-related services, including HESCWeb, a web-based system used to process school and student TAP-related transactions. HESCWeb enables school officials to access individual students' TAP records electronically, identify missing or incorrect data, make corrections, and certify the records. Students can also access HESCWeb, to obtain the information they need to determine whether they are eligible for a TAP grant, to file an application, to review their application data and make any

necessary updates or changes, and to check the current status of their eligibility. HESC contracts with an outside vendor to receive TAP applications and to enter TAP data into EFAN.

B. Audit Scope, Objectives, and Methodology

We audited selected aspects of the general and application controls over TAP's computerized processes, including web-based applications, for the period of April 1, 2001 through December 31, 2002. The objectives of our performance audit were to determine whether HESC had established adequate security over both internally- and externally-initiated TAP system transactions, and whether controls within the TAP system were adequate to ensure compliance with eligibility requirements.

To assess the effectiveness of general controls, we examined the HESC system documentation and records of accounts for users that were no longer active. We reviewed HESC policies relating to passwords, project management, and System Development Life Cycle (SDLC). We tested the password and program change controls in place. We also examined the report of an independent security review of the HESC computer system that was completed in March 2002, and interviewed HESC officials to determine whether weaknesses identified in the review had been corrected. To verify that adequate physical controls were in place, we performed a walk-through of the HESC operating facilities.

To determine the effectiveness of HESC's application controls, we examined documentation of HESC's testing of the outside vendor's accuracy in data entry. We reviewed documentation of TAP eligibility criteria, and met with HESC officials to identify the processes for ensuring that awards are made in accordance with eligibility requirements. We examined HESC's data retention and destruction schedules, and performed a walk-through of on-line transactions to verify the existence of an audit trail. We also interviewed HESC officials to identify the controls installed to protect sensitive data.

Because some of the weaknesses identified by our work could be considered sensitive, we have not included details about them in this report. Instead, we conveyed those findings to HESC officials during the audit.

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 operations of HESC that are included in our audit scope. These standards also require that we understand the HESC internal control structure and its compliance with those laws, rules and regulations that are relevant to HESC operations included in our audit scope. An audit includes examining, on a test basis, the 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 that our audit provides a reasonable basis for our findings, conclusions and recommendations.

We use a risk-based approach when selecting activities to be audited. We therefore focus 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 resources

to identify where and how improvements can be made. Thus, we devote little effort to reviewing operations that may be relatively effective or efficient. 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. Results of Audit

We found that HESC's general and application controls are generally adequate to provide reasonable assurance against unauthorized access to HESC data and systems, and that transactions are being processed accurately. However, we found that, if certain controls were enhanced, there would be greater assurance that only authorized persons would be allowed appropriate access to the network and the Web site, and that all transactions would be authorized appropriately. HESC officials agreed that such controls need to be strengthened and said they would take appropriate actions to address our recommendations.

1. General Controls

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They establish the environment in which application systems and controls operate; include information security measures and access controls such as network vulnerability analyses that could enable HESC to assess various risks, such as unauthorized infiltration into the network and denial of service attacks. General controls also include software controls, application software development and change controls, segregation of duties, and service continuity controls. In the absence of appropriate controls, information and process integrity – as well as public confidence – may be threatened.

Using the HESC Administrative Practices Manual (HESC Manual) and the U. S. General Accounting Office's Federal Information System Controls Manual (FISCAM) as criteria, we evaluated general controls in place at HESC. Our review looked at six areas: security, program planning and management, logical controls, application software change controls, physical controls, and business service continuity.

We also compared HESC policies, procedures, and system settings with recommendations made in the independent security review conducted in 2002, general recommendations by software and hardware vendors and industry leaders, and HESC's own security practices and guidelines. During our audit, we identified several security control weaknesses.

a. Network Risk Assessment

HESC contracted with an outside vendor to identify security vulnerabilities in its computer network. This assessment identified several security vulnerabilities. Although this network risk assessment was completed in March 2002, HESC has not yet fully addressed all findings associated with the assessment. HESC officials indicated to us that they will address all the findings.

b. Granting of System Access Rights to Schools

School employees need to be able to access the HESCWeb system so they can process TAP information for their school. There are more than 2,700 users at 323 schools who have such access. When a school's account is initially set up, school officials designate an individual or individuals empowered to approve new EFAN user accounts for that institution. When the school wants a new user to be authorized, the school's designated authorizer must sign an application for a new EFAN account, certifying that he or she has the authority to approve such access and has instructed the new user on proper usage of the account. When the application is received, HESC staff is required to verify the name of the authorizing individual against a list of approved authorizers. However, our review of 15 EFAN application approvals found that just 6 (40 percent) of the forms bore the signatures of the authorized persons whose names were on file with HESC for their schools.

HESC's Information Security Officer advised us that the list of authorized approvers is not kept current. When HESC receives a new EFAN access application, the new user is processed only if the authorizer's name can be verified against the approved list. If the name is not on the list, Information Security staff contacts the school directly to verify that he or she does have the authority to grant access to others. HESC officials explained that schools are generally not informing HESC in advance about changes in the identities of authorizors. As a result, HESC is unable to ensure that signature authority for granting access to institution accounts on the HESCWeb system has been granted appropriately. In response to our preliminary observations, HESC officials indicated that they will periodically update the signature authority list to ensure that it remains current.

c. Logical Controls over the Network Operating System

When we reviewed selected security settings that might compromise the logical controls over HESCWeb, we identified weaknesses that HESC needs to address if unauthorized access to the system is to be prevented or detected. We reported the details of these weaknesses to HESC officials so they could take corrective action. However, we have not included them in this report. HESC agreed to implement corrective action to address the weaknesses we identified.

d. Password Security

Passwords provide access security only if sufficient controls are present to ensure their confidentiality. If controls are not effective, an individual may impersonate an authorized user and gain inappropriate access to HESC applications. Although the HESC Manual details practices to be utilized for passwords, we found that HESC was not following all of these practices. We reported the details of this non-compliance to HESC officials during our audit, but we have not included them in this report. HESC agreed to implement our recommendation for improving password security.

2. <u>Application Controls</u>

Application controls relate directly to the individual computer programs. Applications controls help ensure that transactions are valid, have been authorized properly, and are being processed and reported completely and accurately. Our review examined the three components of application controls: input, processing, and output.

Input controls are supposed to ensure the accuracy and completeness of the data being entered into the application. Processing controls ensure that authorized transactions are accepted and processed accurately, effectively, efficiently, and completely. For the TAP system, such controls ensure that only eligible students receive TAP, according to the established award requirements. Output controls ensure that output data is complete and accurate, viewable only by authorized personnel, subject to an audit trail, and retained and destroyed appropriately.

Controls over TAP processing and output appear to be adequate. However, we identified one area of input controls in which improvements could be made.

Input Controls Testing

Prior to the processing cycle, HESC performs tests designed to ensure that the outside contractor hired to input information from the TAP applications into the system is performing at the 100-percent accuracy standard. While it is clear that HESC conducted such tests, the documentation of that testing could be improved. For example, HESC did not maintain documentation of the expected results of the testing, the actual results, any problems identified, the cause of these problems, and any corrective action taken. Adequate documentation ensures that testing is consistent from year to year, and provides management and staff with comparable information. When personnel changes occur, such testing documentation can provide new staff with information that will enable them to ensure business continuity. HESC officials informed us that, in response to our preliminary observations, they have taken steps to improve documentation of the testing process.

Recommendations

1. *Address all uncorrected weaknesses identified in the network risk assessment*.

   (HESC officials state that they have already corrected some of the weaknesses identified, and they have set target dates for remediation of the remaining weaknesses.)

2. *Require schools to submit, on a timely basis, any changes in signature authority for account authorization, and to update the signature authority listing whenever personnel changes occur.*

   (HESC officials state that they are conducting a survey of TAP schools and will require certifying officers to provide the names and titles of their financial aid professionals. HESC will verify this information and send letters to schools each quarter to confirm the status of staff with signature authority.)

3. *Adjust the security settings over the network operating system to the recommended levels.*

   (HESC officials state that they have adjusted the settings to require all users to change their passwords at the proper time intervals.)

4. *Comply with all password practices described in the HESC administrative manual.*

(HESC officials state that they have improved security procedures for sending passwords for new accounts to schools and for storing administrative passwords. Also, HESC has implemented a procedure to verify employee identity prior to a password reset.)

5. *Maintain formal documentation of HESC's efforts to test application data entered by the data entry contractor. At a minimum, this documentation should include the expected results of the testing, the actual results, the problems identified, the cause of these problems, and any corrective actions taken.*

(HESC officials agree with recommendation number 5 and state that they have implemented procedures to maintain the test data, including the expected and actual results, and to document actions taken.)

We prepared several other recommendations based on additional findings that we discussed with agency officials during the audit. However, due to the sensitive nature of the issues involved, the details of these findings are not included in this report.

A draft copy of this report was provided to HESC officials for their review and comments. Their comments have been considered in preparing this final report and are included as appendix A. HESC officials agree with our recommendations.

Within 90 days after the final release of this report, as required by Section 170 of the Executive Law, the President of HESC 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 Brian Mason, Abe Fish, Melissa Little, Adrean Kreig, Jessica Feltman, Melissa Clayton, and Marticia Madory.

We wish to thank the management and staff of the Higher Education Services Corporation for the courtesies and cooperation extended to our auditors during the audit.

Very truly yours,

Steven E. Sossei
Audit Director

cc: Marvis Warren
Deirdre Taylor

GEORGE E. PATAKI
GOVERNOR

NEW YORK STATE
HIGHER EDUCATION SERVICES CORPORATION
99 WASHINGTON AVENUE
ALBANY, NEW YORK 12255
518/474-5592 Fax 518/474-5593
WWW.HESC.ORG

PIERRE L. ALRIC
ACTING PRESIDENT

April 17, 2003

Mr. Steven E. Sossei
Audit Director
Office of the State Comptroller
110 State Street
Albany, NY 12236

RE: TAP Application Process
Report 2002-S-41

Dear Mr. Sossei:

Enclosed for your information and review is the Higher Education Services Corporation (HESC) response to the recommendations made as a result of your audit conducted on the TAP Application Process for the period of April 1, 2001 through December 31, 2002. I am pleased with your conclusion that HESC's general and application controls are generally adequate to provide reasonable assurance against unauthorized access to HESC data and systems, and that transactions are being processed accurately.

I would like to express my appreciation for the efforts and the professionalism which were exhibited by the Office of the State Comptroller staff who were assigned to this audit. Please do not hesitate to contact me if you require additional clarification of any of the information presented herein.

Sincerely,

Pierre L. Alric
Acting President

PLA/maw/nh
Enc.

Appendix A

RESPONSE TO REPORT OF AUDIT
OF NYS HIGHER EDUCATION SERVCIES CORPORATION'S
TAP APPLICATION PROCESS

Recommendation 1: Address all uncorrected weaknesses identified in the network risk assessment.

Response:

- Four high risk weaknesses were identified. Three have been corrected . The remaining weakness will be corrected when HESC migrates the TAP reports and forms application to the OS/390 platform in Spring 2003.
- Five medium risk weaknesses were identified. Three have been corrected. The remaining two weaknesses are targeted for remediation by October and December 2003.
- The risk assessment directed that low risk findings "should be noted and implemented at a later date but may not pose a real threat to the network and connected systems at this time." HESC has raised awareness of secure web programming through training and is publishing guidelines for secure web coding for programmers and consultants. HESC will correct the significant low risk findings as new code is developed or existing code is modified. We anticipate that these findings will therefore be corrected by Spring 2004.

Recommendation 2: Require schools to submit, on a timely basis, any changes in signature authority for account authorization, and to update the signature authority listing whenever personnel changes occur.

Response: HESC is conducting a TAP Survey, completed by the Certifying Officer, giving names and titles of financial aid professionals. The security procedure will require verification to that information. Each quarter, a letter confirming the signer's status is sent.

Recommendation 3: Adjust the security settings over the network operating system to the recommended levels.

Response: The settings have now been set to require all users to change their password at the proper
interval.

Recommendation 4: Comply with all password practices described in the HESC Administrative Practices Manual.

Response:

- HESC has implemented a new procedure to address the recommendation regarding sending unencrypted ID's and passwords to schools. When a school account is set up, an e-mail is sent asking the recipient to call the HESC Help Desk to obtain the password. Verification information is asked when the user calls the Help Desk.
- The condition that administrative passwords were not properly stored in the security office has been corrected. All passwords are now stored and properly labeled.

- HESC has implemented a procedure, regarding the recommendation for verification of employee identity prior to password reset, which requires the Help Desk to also verify a PIN.

Recommendation 5: Maintain formal documentation of HESC's efforts to test the TAP application data entered by the data entry contractor. At a minimum, this documentation should include the expected results of the testing, the actual tests, the problems identified, the cause of these problems, and any corrective action taken.

Response: HESC management agrees with the finding and implemented procedural changes, which were, used in the testing and approval of the NCS programs in January and February of this year. Specifically, the Assistant Director of Grants and Scholarship created and will maintain the test data used, as well as a test data matrix. The test data matrix includes each example tested, the expected result, the actual result, and action taken. This year all transactions processed as expected. This testing procedure will be used for testing in future years.