Thomas P. DiNapoli
COMPTROLLER

OFFICE OF THE
NEW YORK STATE COMPTROLLER

DIVISION OF STATE
GOVERNMENT ACCOUNTABILITY

CITY UNIVERSITY OF NEW YORK

EMPLOYEE ACCESS TO THE STUDENT INFORMATION MANAGEMENT SYSTEM AT SELECTED CAMPUSES

Report 2007-S-23

AUDIT OBJECTIVE

Our objective was to determine if CUNY's controls over employee access to the Student Information Management System were adequate at selected campuses.

AUDIT RESULTS - SUMMARY

The City University of New York (CUNY) is the largest municipal college system in the United States. It serves more than 226,000 degree-credit students and 230,000 adult, continuing and professional education students. For the 2007-08 fiscal year, CUNY's operating budget exceeds $1.6 billion. The majority of CUNY campuses use the Student Information Management System (SIMS) to track student information. SIMS is a mainframe application which contains student personal information, account balances, course selections, grades and loan information.

CUNY officials have taken meaningful steps to enhance information technology (IT) security in recent years. For example, CUNY established an IT Steering Committee, hired an Information Technology Security Officer (ITSO) to oversee an Information Security Team, and allocated $2 million to IT security initiatives. In addition, CUNY issued its formal Information Technology Security Policies (Policies) in August 2006.

However, the colleges we visited did not fully comply with the Policies, and as a result, there were significant weaknesses in the controls over SIMS access. Because of the weaknesses, unauthorized users could have access to SIMS; and some authorized users might have inappropriate access to certain types or levels of SIMS information. We concluded that the ITSO and/or the Information Security Team should make periodic site visits to CUNY's campuses to help ensure that campus officials are complying with the prescribed Policies and limit SIMS access appropriately.

The Policies prescribed a number of requirements that colleges must follow to secure their computerized resources. For example, the Policies prohibit colleges from issuing generic user IDs and multiple IDs to users. However, at the four selected colleges we found that 74 users had more than one user ID, and there were 216 generic IDs.

The Policies further require computerized user accounts to be deactivated timely whenever someone's employment with CUNY ends. However, we noted that 60 former employees at four campuses we reviewed (Hunter, Baruch, City and Medgar Evers) still had SIMS access after they left CUNY. The Policies also require users to change their passwords at least every 90 days. However, we interviewed 55 employees at three campuses (Hunter, Baruch, and City) and found that 35 of them had never changed their SIMS password.

According to the Policies, users should only access computerized information that is necessary to perform their job functions. However, we determined that 21 of the 55 employees we interviewed had the ability to change grades, adjust student account balances, or add and remove stop codes, although these employees did not need such capabilities. (Stop codes are used to deny student registration for reasons such as past-due account balances.)

Our audit report contains 13 recommendations to help CUNY strengthen SIMS access controls. In their response to our draft report, CUNY officials generally concurred with our recommendations. They indicated the specific actions that they have

already taken and will be taking to implement them.

This report, dated February 8, 2008, is available on our website at: http://www.osc.state.ny.us.
Add or update your mailing list address by contacting us at: (518) 474-3271 or
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

BACKGROUND

The City University of New York (CUNY) is the largest municipal college system in the United States. It consists of eleven senior colleges, six community colleges, and several other specialized and professional schools. CUNY serves more than 226,000 degree-credit students and 230,000 adult, continuing and professional education students. Governed by a 17-member Board of Trustees, CUNY employs about 6,100 full-time faculty members. For the 2007-08 fiscal year, CUNY's operating budget totaled more than $1.6 billion.

In recent years, CUNY has increased its commitment to IT security. In October 2005, CUNY officials hired an ITSO. Subsequently, they established a University Information Security team. The ITSO works with each CUNY campus through the University IT Steering Committee, which is comprised of the Chief Information Officers and Vice Presidents of Finance and Administration for each college. The IT Steering Committee approved a comprehensive IT Security Strategic Plan and has allocated more than $2 million for projects addressing IT security issues.

The ITSO reviewed CUNY's IT security policies. Based on this review, CUNY officials issued the Policies (on August 30, 2006) to be promulgated immediately to all CUNY offices and campuses. The Policies included guidance on the use, creation, and severance of user IDs; standards pertaining to the formation and use of generic and duplicate user IDs; and requirements for the maintenance of user passwords. Each College's Vice President of Finance and Administration has primary responsibility for compliance with the Policies, including the resolution of instances of non-compliance. The colleges are also required to conduct internal reviews each semester to ensure that they are following the Policies, and college officials must submit letters to the ITSO attesting to the performance of such reviews. However, CUNY Central Office still maintains a significant oversight role with regard to campus IT security.

The majority of CUNY campuses use SIMS to track student information. SIMS is a mainframe application which contains student personal information, account balances, course selections, grades and loan information. Within the next few years, CUNY officials plan to replace the 25-year old SIMS with a system that is expected to have many security and other improvements. In the interim, issues related to hardware and backup are handled centrally by the CUNY Office of Computing and Information Services, while each college grants its users access to SIMS, including the type of access that each user should have. College registrars are generally the SIMS data owners and approve SIMS access requests.

To determine whether colleges were complying with the new Policies and other best practices, we judgmentally selected four colleges for audit. We selected a sample of senior colleges with high and low student to SIMS user ratios. The colleges selected were Hunter (836 SIMS user IDs), Baruch (505

user IDs), City (1,039 user IDs) and Medgar Evers (347 user IDs) colleges. We obtained the most current SIMS user listings from these colleges during the period of May 22, 2007 to July 17, 2007. At City College, the most current user listing had not been updated since January 2006. We analyzed and tested the user listings for each college and conducted employee interviews at Hunter, Baruch and City College. We did not include community colleges or specialized and professional schools in our review. Our audit period was from May 1, 2006 to August 16, 2007.

AUDIT FINDINGS AND RECOMMENDATIONS

Analysis of SIMS User Listings

Effective access controls require that users' access to an entity's computerized resources be linked to specific individuals to prevent and detect unauthorized transactions. Also, access should only be granted to current employees unless there is a valid and documented reason to do otherwise, and access should be terminated promptly when employees leave the organization. These controls are particularly important when the users are assigned a high level of access, such as the ability to update student information within SIMS. However, we found that colleges maintained duplicate and generic IDs, and non-CUNY employees and separated employees had access to SIMS.

Duplicate and Generic User IDs

The Policies state, "Users of computerized systems should have no more than one individually assigned user ID, clearly identifiable to a user." Further, the Policies state that generic named or group user IDs are not permitted. To determine if employees had more than one SIMS user ID, we summarized the SIMS user listings provided by each of the four selected colleges by user ID, and then we searched for those user names that had more than one SIMS ID. We found that 74 employees had more than one SIMS user account. These included 33 employees at Baruch College, 35 employees at City College, and 6 employees at Hunter College.

According to Baruch College officials, some users are only able to print to specific printers. Consequently, some of these users requested additional user IDs to facilitate printing on other printers. It should be noted that Brooklyn College officials indicated they receive many requests from their employees to obtain an additional ID when they need to print to another printer. However, in these instances the IT personnel make a change to the SIMS printer table for those users, thereby avoiding the need for multiple IDs. We believe this solution should be shared with CUNY IT managers at other campuses to minimize the need for multiple IDs for individual staff.

Prior to the conclusion of our fieldwork, officials from Hunter College advised us that they eliminated all six of their duplicate user IDs we identified. They attributed several of these instances to employee transfers within the campus. The transfers resulted in new user IDs for the employees. However, the employees' old user IDs, from their previous work locations, had not been canceled. Based on Hunter's comments, we conclude that CUNY should ensure that campuses have adequate procedures to cancel the old IDs of employees that transfer from one work location to another within a campus or the overall CUNY system.

Generic IDs are not assigned to a specific individual and are typically used by multiple users. To determine if the SIMS user lists

contained generic IDs, we reviewed each of the four colleges' user lists and identified those IDs not assigned to specific persons. We found 216 generic user IDs: 15 at Baruch College; 12 at Medgar Evers College and 189 at City College. Baruch College personnel informed us that they will deactivate their generic IDs. City College officials told us their generic IDs are actually "unassigned IDs." Medgar Evers College officials have taken no action and believe the ID's are necessary. However, the ITSO informed us that generic IDs of any sort are strictly prohibited.

When colleges allow duplicate and generic accounts to be issued, accountability for the actions of SIMS users is diminished.

Separated and Non Employee Access to SIMS

The Policies state, "Access to computerized systems must be severed prior to or upon the last date of employment." We compared the user listings of active SIMS accounts for each of the four colleges noted above, with the names of employees who were separated from employment at each college, according to the New York State payroll system. The payroll records used in our testing indicated those employees that were terminated, resigned, retired, deceased or on leave between September 2006 and June 2007. Our objective was to determine whether these former or inactive employees had their SIMS access privileges terminated.

We found that 60 former CUNY employees had active SIMS user accounts after their termination dates. These included 12 users from Hunter College, 28 users from City College, 18 users from Baruch College, and two users from Medgar Evers College. Of the 60 former employees who still have an active SIMS user ID, 22 users were terminated for reasons including seasonal or temporary employment; 22 users had resigned; 13 users retired; one user was formerly an adjunct professor; and two users were deceased. Furthermore, 17 of the 60 discontinued employees had accounts that granted them high levels of SIMS access. Each of these former employees had Stop Code Update capability (used to deny student registration for reasons such as past-due fees), the ability to adjust student SIMS account balances, and/or grade change update capability.

We also found another 22 employees who were on a leave of absence at the time of this review, but still had active user IDs. At the time of our audit fieldwork, CUNY had not developed a policy to determine when officials should deactivate the user accounts for employees on leave. Although there may have been justifications for some of these employees, for others (particularly those on extended or indefinite leaves) there could be little or no justification for their continuing SIMS access. CUNY officials responded that they will determine whether there are alternatives for modifying access privileges for employees on extended leave who do not require their normal levels of access.

If individuals who are no longer active employees continue to retain access rights to SIMS, they may inappropriately obtain confidential data; and there is an increased risk that they can use the system for improper purposes.

Best practices also dictate that all SIMS users should be employees of the college, unless there is a valid reason otherwise (i.e. consultants). According to the SIMS user listings provided to us, Hunter, Baruch, City and Medgar Evers Colleges had a combined total of 1,163 user IDs with the ability to change grades, adjust student account balances, or add or remove stop codes

through SIMS. We compared 200 randomly selected users who had at least one of these user privileges, from all four colleges, with the New York State payroll records for the periods noted above. Our objective was to determine whether these users were current CUNY employees.

Of the 200 users selected for our sample, we could not find 10 individuals on the CUNY payroll. These included two Baruch College users, seven City College users and one Medgar Evers College user. City College officials indicated that three users not found had resigned or retired during 2005, and one employee resigned after June 2007. A City College IT official informed us that the user listing had not been updated since January 2006. No explanations were offered for the remaining users. We referred this to CUNY officials for follow up.

If individuals who are no longer active employees (or who were never employed by CUNY) have access rights to SIMS, they may inappropriately obtain confidential data, and there is an increased risk that they can use the system for improper purposes.

Recommendations

To the Colleges:

1. Comply with CUNY's Policies, and remove all generic and duplicate SIMS user IDs.

2. Ensure that user SIMS accounts are disabled timely, upon an employee's separation or long term absence from employment.

3. When an employee transfers from one operating unit to another, resulting in the creation of a new user ID for that employee, ensure that the employee's old user ID is terminated.

4. Ensure that only current CUNY employees have access to SIMS, unless there is a valid reason otherwise. Adequately document the justification and approval of SIMS access granted to individuals who are not CUNY employees.

5. Ensure that user listings are updated on a regular basis.

To CUNY Central Office:

6. Provide the technical guidance needed to enable the campuses to change SIMS printer tables, and thereby, help minimize the issuance of multiple user IDs to individual employees.

7. Ensure that colleges are aware of the need to address issues, such as the use of multiple IDs and the disabling of accounts for terminated employees.

8. Develop and implement a policy for determining when colleges should disable the accounts of employees who are on extended leave.

SIMS Password and User Access Controls

User passwords are generally the first controls that an entity uses to ensure that only authorized individuals have access to its computerized systems and information. Moreover, it is essential that employees receive the least level of access necessary to perform their required job functions. However, we found that some SIMS users did not periodically change their password, and college officials granted access privileges to certain employees that were beyond the

access levels required for these employees to do their jobs.

SIMS Password Controls

Passwords are important access controls intended to prevent unauthorized access to computer resources. CUNY's Policies state, "All passwords must be changed at least every 90 days. Accounts which have special access privileges must be changed at least every 60 days." However, we found weaknesses in SIMS password controls. The SIMS system currently does not automatically require users to change their passwords periodically. Consequently, some users rarely (if ever) change their passwords. Although CUNY Central Office officials were aware of this shortcoming within the SIMS system, compensating controls had not been implemented. We conclude that CUNY officials should implement compensating procedures, such as training employees to change passwords as required and notifying supervisors to require compliance with this requirement.

Generally, SIMS users had been not informed of the importance of changing their passwords (or otherwise trained/directed to do so). From three colleges, we randomly selected 55 of the 1,054 SIMS users who had the ability to change grades, adjust student account balances, or add or remove stop codes through SIMS. These consisted of 25 users at Hunter, 20 users at Baruch and 10 users at City Colleges. We interviewed each of these employees and inquired about SIMS password changes. Thirty-six of these employees stated that they never received computer security training or notifications by supervisors or IT personnel to change their passwords. As a result, we found that 35 of these 55 employees had never changed their SIMS password. If users do not change their passwords periodically, this increases the risk of inappropriate access to automated information systems.

SIMS User Access Privileges

Colleges are responsible for ensuring that all SIMS users have legitimate business reasons for accessing information. Therefore, the Policies state "Access to non-public University data must be limited to a strict need to know, consistent with the user's job responsibilities…" Since much of the information in SIMS is confidential, there are different levels of access provided to people, depending on their job function. Requests for access to SIMS are generally sent to the school registrars, who review the request and approve or disapprove them based on this criterion. Approved requests are sent to the IT department to set up the accounts.

We further interviewed the 55 SIMS users noted previously to ascertain the job functions of each employee, and how they use SIMS during the course of their work. We then sought to determine whether the access privileges granted to them were necessary to perform their duties. The 55 employees have the ability to change grades, adjust student account balances, or add and remove stop codes. However, 21 of these employees indicated their jobs did not require them to have certain access privileges that had been established for them. The 21 employees included nine at Hunter College, ten at Baruch and two at City College.

At Hunter College, for example, a Coordinator of the Student Ambassador Program (involved with recruitment and outreach) only uses SIMS for inquiry purposes. Nevertheless, this employee had stop code update privileges. At Baruch College, a Transfer Evaluation Coordinator (who oversees students who transfer to Baruch) uses SIMS screens only to help with

transfer credits and student IDs. However, this employee also had grade change update ability. Also, a Secretary in the Bursar's Office at City College uses SIMS only to find students' addresses, but nevertheless also has stop code update access. Baruch College officials responded that four users requested (and were given) one-time access to certain functions. However, these access privileges were not terminated when the employees in question no longer needed them.

When individuals have access to SIMS, or certain SIMS privileges, that are not needed to perform their job responsibilities, they may have inappropriate access to confidential student information and may compromise student privacy. Moreover, there is an increased risk that improper changes could be made to student records.

During our visit to City College, we also noted that college officials had not implemented the policy regarding the restriction of re-using user IDs. The Policy states that "user IDs must not be re-used or re-assigned to another individual at any time in the future." Moreover, the NYS Office for Technology's Best Practice Guideline G07-001 states, "User IDs shall be unique. Therefore, User IDs may not be re-used and will be archived when the user is deprovisioned." City College officials indicated they re-use the same SIMS IDs because it is easier for the IT Department to disable an account by changing the password instead of deleting the account and adding a new account. City College Officials indicated that they lack the resources within the IT Department to constantly add and delete user accounts. However, during a visit to Brooklyn College, officials indicated that it takes only five minutes to disable access capabilities when deleting accounts, and no more than an hour to add a new user account. The re-use of user accounts makes it more difficult to control and limit access rights, and it hinders the ability to track user activity.

Recommendations

To the Colleges:

9. Formally notify all SIMS users of the need to change their passwords periodically and provide training as necessary to employees regarding this matter. Require supervisory personnel to verify that employees have changed passwords, consistent with prescribed policies.

10. Ensure that all SIMS users are given only the access privileges that are required to perform their job functions.

11. Comply with CUNY's Information Technology and Security Policies restricting the re-using of user IDs.

CUNY Central Office Oversight

CUNY colleges are required to submit attestation letters to the Central Office each semester confirming compliance with the Policies' requirement for periodic access reviews. At the time of our audit fieldwork, all 11 of CUNY's senior colleges had submitted their letters for reviews purported to have been performed during the Fall 2006 term. We reviewed the letters for the four colleges and found that:

- Baruch College, officials cited generic and duplicate accounts as concerns.

- City College officials stated that they do not re-use user IDs. However, this was contrary to our own site visit findings, as noted previously. The ITSO informed us that printing issues

are the result of the age of the SIMS system and should be resolved when the new system is employed in the future. However, we noted, as detailed previously in this report, that Brooklyn College solved this problem by making changes to SIMS printer tables, as necessary. Moreover, the operational replacement of SIMS will likely take several years to complete. Consequently, we believe that CUNY Central Office officials should takes steps to ensure that all campuses have the technical ability to change system printer tables, as necessary, to obviate the need for employees with multiple user IDs.

As noted previously, CUNY officials have taken significant steps in recent years to improve IT security controls, including those over SIMS access. These steps include the formation of an IT Steering Committee and an Information Security Team, the appointment of the ITSO, and the issuance of the Policies. However, our review indicated that all four colleges included in our audit (Hunter, Baruch, City and Medgar Evers) did not consistently comply with certain aspects of the Policies. Furthermore, formal site visit reviews of campus IT security activities by the ITSO and Information Security Team were limited. Consequently, based on the results of our campus reviews and the limitations in Central Office oversight, we believe that there is increased risk of non-compliance with the prescribed IT security standards at the campuses we did not visit. Although campus officials have primary responsibility for compliance with the Policies, we concluded that CUNY Central Office officials need to strengthen their oversight of campus IT security programs. Such oversight could include site visits to campuses and reviews of files/documents prepared by campus staff to perform the required periodic access reviews.

Recommendations

To CUNY Central Office:

12. Direct the ITSO and/or the Information Security Team to perform periodic site visits to the campuses to verify compliance with the Guidelines. Document the results of the site visits and share them with campus officials, as appropriate.

13. On a sample basis, examine the files/documents prepared by campus IT staff to perform the required periodic access reviews, as prescribed by the Guidelines.

AUDIT SCOPE AND METHODOLOGY

We conducted our performance audit in accordance with generally accepted government auditing standards. We audited CUNY's SIMS access controls at four selected colleges and the CUNY Central Office for the period May 1, 2006 to August 16, 2007. Our audit focused primarily on the access controls in place to secure the SIMS system. We reviewed policies and procedures; analyzed college user reports and compared them with payroll records and interviewed SIMS users. We also met with information technology employees, bursars and registrars.

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. 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 functions do not affect our ability to conduct independent audits of program performance.

AUTHORITY

The audit was performed 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.

REPORTING REQUIREMENTS

We provided draft copies of this report to CUNY officials for their review and formal comment. We have considered CUNY's formal comments in preparing this report and have included them as Appendix A. CUNY officials generally concurred with our recommendations, and they indicated the specific actions that they have already taken and will be taking to implement them.

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

CONTRIBUTORS TO THE REPORT

Major contributors to the report include Brian Mason, Abe Fish, Keith Dickter, Nicole Van Hoesen, Shanna Mogan and Ron Pisani.

APPENDIX A - AUDITEE RESPONSE

The City University of New York

Vice Chancellor for Budget and Finance
Office of Internal Audit and Management Services
230 West 41st Street, 5th Floor
New York, NY 10036
Tel: 646-746-4290
Fax:646-746-4299

January 8, 2008

Mr. Steven E. Sossei
Audit Director
Office of the State Comptroller
Division of State Government Accountability
110 State St., 11th Fl.
Albany, NY 12236

Re: Audit Report 2007-S-23, draft November 29, 2007

Dear Mr. Sossei:

I am writing to respond to the findings and recommendations contained in the above-captioned audit report on the OSC audit of access controls over the CUNY Student Information Management System (SIMS).

I would first like to emphasize that the University takes information technology and appurtenant systems access matters very seriously, as is in part evidenced by the significant investment the University is making in the replacement of its aging legacy application systems with a state-of-the-market, fully-integrated Peoplesoft ERP system from Oracle Corporation. This major initiative will replace the existing SIMS system and will introduce many security capability improvements that were not possible technically, not required by regulation, or designed into a system that is now over 25 years old.

In the intervening period prior to full implementation of the ERP system, the University Information Security Program has instituted many procedural improvements that address the SIMS system deficiencies and has mandated compliance with these procedures.

The following are our comments and responses regarding the audit report recommendations:

Audit Findings and Recommendations

To accomplish issues raised by the audit findings and recommendations, the ITSO presented formal guidance to the IT Steering Committee on September 20, 2007 and distributed written material on September 21, 2007 to the Committee for those who were not present. In addition, the same written guidance was distributed to the IT Steering Committee and all College IT Directors on November 12, 2007 when we requested submission of fall semester security attestations.

The following written guidance, consistent with approved information security Policy, was provided. A cross reference to the recommendation number in your audit report is noted after each item of guidance:

1. Generic accounts are not be used. All user accounts must be assigned individual accountability. We also instructed the Committees to use individually assigned user IDs for remote College registrar department employees and to eliminate the use of generic accounts for such purpose. In addition, all service accounts historically added to the College SIMS instances by Central Office have now been assigned individual accountability (#1).

2. Business users with accounts to SIMS are limited to one user ID. We also instructed the Committees to eliminate the use of unassigned (or "off the shelf ready") user IDs and to not reuse user IDs (#1, #11).

3. Access to SIMS must be restricted to current employees of CUNY and its related entities and any former or non-current employees of CUNY and its related entities must be removed on a timely basis. Accounts belonging to long-time absent employees must also be removed (or suspended) on a timely basis (#2, #4).

4. Access to non-public SIMS data must be maintained consistent with the user's job responsibilities and adjusted on a timely basis if job responsibilities change (#3, #10).

5. IT Security Policies were amended in October 2007 to include the following requirement: "Documentation, showing the review steps taken in arriving at the attestation, must be retained in the office of the Vice President of Administration or the equivalent at the College or in the Central Office department and be made available for further review by the University Information Security Officer and internal/external audit entities as appropriate." Updated user listings are expected to be part of this documentation portfolio (#5, #13).

6. The ITSO instructed the IT Steering Committee to change SIMS printer locations on user IDs as needed and advised the Committee to model their College procedure against the Brooklyn College procedure (#6).

7. The ITSO presented formal guidance on audit report issues to the IT Steering Committee on September 20, 2007 and distributed written material on September 21, 2007 to the Committee for those who were not present. In addition, the same written guidance was distributed to the IT Steering Committee and all College IT Directors on November 12, 2007 when we requested submission of fall semester security attestations (#7).

8. We will examine any further alternatives that may exist for modifying system access for those employees who are on extended leave and do not require all of their normal account privileges and introduce policy changes as appropriate (#8).

9. Passwords must be changed regularly in accordance with Policy. College officials were instructed to implement procedural controls for changing SIMS passwords which includes line management oversight for compliance with this procedure (#9).

10. The ITSO and the Information Security Team will collaborate with CUNY Internal Audit to provide oversight of the campuses, including periodic site visits, to help ensure that campus officials are complying with the prescribed Policies and limit SIMS access appropriately. It is emphasized that responsibility and accountability for adhering to and maintaining compliance with these procedures, however, is assigned, by procedure, to the colleges' Vice President of Finance/Administration. We have instructed our newly hired IT Security Policy & Compliance manager to visit campuses, to provide further guidance, review documentation and confirm state of reported compliance (#12, #13).

In addition, we have completed or have planned the following activities:

1. CUNY issued its formal Information Technology Security Policies in August 2006 and updated it in October 2007. The revisions included clarifications from our internal practical experience with these Policies over the past year and recommendations made as a result of this audit.

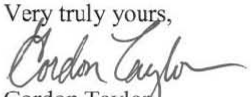
2. We will continue to use the IT Steering Committee, IT Directors Committee and the Information Security Managers Forum to share best practices. We agree that such forums serve an important information gathering/dissemination and best-practices sharing purpose, and we will continue our efforts to provide such opportunities to our colleges.

Summary

The University believes that some of the audit findings and recommendations overshadow the very significant achievements the University has procured with respect to its systems and security controls. However, we note that some of the findings are consistent with our own assessment of where improvements are needed. It is our position that we are steadfastly addressing deficiencies wherever they may exist and are making measurable improvements.

Within the past two years, the University created the Information Technology Security office and issued and updated IT Security procedures, both of which were additive measures with respect to the University's efforts in improving system integrity. We have also embarked on one of the largest ERP implementations ever recorded in an effort to improve our systems and related controls. These efforts have required that we make the difficult decision to redirect scarce resources to information technology, but we realize that such an investment in our systems bolsters the quality of our academic and programmatic offerings. We believe that our efforts illustrate the high regard in which we hold information technology systems and the security controls that will enable us to maintain system integrity, thus protecting our investment in these systems.

Very truly yours,



Gordon Taylor
Director

cc: Chancellor Matthew Goldstein
Executive Vice Chancellor Allan H. Dobrin
Vice Chancellor Ernesto Malave
Associate Vice Chancellor and CIO Brian Cohen
IT Security Director Carl Cammarata

IA#2072