CONNECTICUT STATE
COLLEGES & UNIVERSITIES
BOARD OF REGENTS FOR HIGHER EDUCATION

BOR INFORMATION TECHNOLOGY COMMITTEE
Thursday, September 19, 2013, 3:00 p.m. to 4:30 p.m.
61 Woodland Street, Hartford, CT 06105
2nd Floor, Room 238

AGENDA

1. *Approval of Minutes from June 7, 2013

2. BOR CIO Report

3. Discussion of IT Governance Model

4. *Discussion/Approval of Security Resolution

5. *Discussion of Annual Information Security Reporting Process

6. Move to Executive Session

    a. Discuss Personnel Issues

    b. Discuss Security Matters

7. Adjournment

*=attachment

BOR INFORMATION TECHNOLOGY COMMITTEE

Friday, June 7, 2013, 1:00 p.m. to 3:00 p.m.
61 Woodland Street, Hartford, CT 06105
2nd Floor, Room 238
REVISED Minutes

COMMITTEE MEMBERS PRESENT
Nickolas Donofrio, Chair
Michael Pollard
Matthew Fleury

BOR STAFF
Wendy Chang, Chief Information Officer
Joe McAuliffe, Director, BIS BOR
Jeff Clark, Information Security Program Officer
Karen Stone, Director of Internal Audit
Ernestine Weaver, In House Counsel
Victoria Lee Thomas, ITS Support Staff

UNIVERSITY AND COLLEGE REPRESENTATIVES
George Claffey, CIO, COSC
Joseph Danajovits, IT Director, NWCC
Tom DeChiaro, Interim CIO, WCSU
James Estrada, CIO, CCSU
Stephen Goetchius, IT Director, TRCC
Barry Grant, IT Director, MCC
Lynn Gregor, IT Director, ACC
Pablo Molina, CIO, SCSU
Joe Tolisano, CIO, ECSU

CALL TO ORDER

With a quorum present, Committee Chair Donofrio called the meeting to order at 1:05 p.m.

1.   Approval of Minutes from April 5, 2013
The minutes of the April 5, 2013 meeting were unanimously approved on a motion by Regent Fleury, seconded by Regent Donofrio.

2.   BOR CIO Report
Committee members were provided with a quarterly project management dashboard which detailed construction, non-construction and of completed projects for FY 2013. Wendy Chang highlighted the following projects:

- On-Line student payments (debit card & payment plans) - Product has been purchased and installed. The implementation team is working with the product. 6/5/13: All CCC's will have this live by July.

- College to College Transcript Exchange - Created an RFI with a group of Registrars, Admissions and IT people from the ConnSCU system to pursue a solution to facilitate transcript exchange amongst the 17 ConnSCU institutions as well as outside institutions.

- OpenScholar - Public website for faculty to promote their academic work. Working with Housatonic to bring in departmental site. 6/5/13: Faculty has been invited - response is low.

- Cisco Telepresence - Integration and project almost complete. 6/3/13: No status change.

- Enterprise Network Project - This project is a collection of many smaller projects. Details can be provided upon request. See Enterprise Network & Voice upgrade sheet for status update on individual projects.

- Wireless Network Upgrade in Residence Halls - 4/11/13. Kickoff meetings held at each of the universities. CES is currently working on the design and bid documents for WCSU and SCSU. 6/3/13: CES begun working on the design & bid documents for CCSU. Currently, reviewing preliminary documentation for SCSU & WCSU.

- Construction - ITBD Telecom Upgrade - New MDF & IDF 4/12/13. The construction phase of the project is complete. Awaiting purchase and installation of the telecom server

- Student E-mail - Project completed.

- Construction - Housatonic and Naugatuck Valley Community Colleges Manufacturing Labs - Project completed. Governor's ribbon cutting ceremony scheduled for 10/3/12. Production to begin 10/18/12.

- Telecom Voice Upgrade - VoIP at SO - VoIP upgrade for Avaya PBX completed last year and most phones at 39 Woodland Street are IP phones. Remaining non-IP phones at 39 Woodland are changed to IP phones as staff change or move.

- Data Backup Storage & Disaster Recovery Phase I - All planned work for the Exagrid Project has had completed. New devices installed at SCSU and CCSU. The system is in full production.

Wendy also noted that these are just a glimpse of the projects the IT department is working on; there are over 100 projects; many of which are not listed here and these projects are being performed with fewer IT staff since the merger. She concluded by stating all vendor contracts are in the process of being renegotiated and the savings are about $1 million dollars starting FY14. Regent Donofrio indicated that he would like to review the plans for all major projects going forward.

Pablo Molina requested a legend or symbols be added to the dashboard report indicating completed and or pending projects. Regent Pollard added that he would like to see the dashboard projects prioritized, identifying critical projects at a glance. This item will be added to the agenda for the September 11, 2013 meeting.

On behalf of the Board of Regents, Regent Donofrio thanked Dr. Wendy Chang for her service and dedication and wished her well on her future endeavors.

3. Approval of IT-001 and IT-002 Revisions
There were several questions regarding IT 001 and IT 002 prior to the revisions by Counsel Weaver. The faculty still has questions and concerns regarding the privacy act section of the policy and after a productive discussion, the CIOs suggested tabling the approval of this policy until the October meeting. That will give ample time for the faculty to review the policy once again and address any lingering issues with the CIOs. Chairman Donofrio motioned to table the policy until October. Regents Pollard and Fleury agreed.

4. Approval of Expedited Approval Process for Security Standards
The aforementioned proposed processes authorize the BOR President to implement a process to expedite the development, approval and promulgation of standards, procedures and guidelines in connection with information security. Regent Pollard stated that the Administrative Committee should also be informed of this process as a courtesy. With respect to the issue of which policies should be followed while new processes are being developed, Counsel Ernestine Weaver stated that in accordance with the Board of Regents Policy, all policies governing the respective constituent units remain in effect unless amended or rescinded by the BOR, so colleges should continue to follow CCC policy and the universities should continue to follow CSU policy. Regent Pollard made a motion to move forward, Regent Fleury seconded motion.

5. Move to Executive Session
Committee Chair Donofrio requested a motion to go into Executive Session for the purpose of discussion concerning the review of the Information Security Program Implementation. Wendy Chang, Joe McAuliffe, Jeff Clark, Ernestine Weaver, Karen Stone, CIOs and IT Directors were asked to stay in the meeting. *Regent Pollard approved a motion, seconded by Regent Fleury.*

6. Adjournment

RESOLUTION

concerning

The Design, Implementation Operational Management and Assurance/Compliance of the Information Security Program for the Board of Regents of Higher Education

[Month], [Day], 2013

WHEREAS,   The Board of Regents (BOR) for the ConnSCU recognizes that unauthorized disclosure of certain personal information is prohibited by various state and federal statutes, and

WHEREAS,   The Board of Regents (BOR) for the ConnSCU recognizes that the implementation of an Information Security Program is mandated by state and federal statutes, including but not limited to: Connecticut General Statutes Section 36a-701b et seq., Family Educational Rights and Privacy Act (FERPA) 20 USC §1232g , Gramm-Leach-Bliley Act (GLBA) 16 USC §314, e-Discovery, Health Insurance Portability and Accountability Act (HIPPA), and Electronic Communication Privacy ACT (ECPA) 18 USC § 2510, and

WHEREAS,   The Board of Regents (BOR) for the Connecticut State Colleges and Universities (ConnSCU) recognizes that information security needs to address availability, confidentiality and integrity of ConnSCU information whether in electronic or paper form.

WHEREAS,   To meet the missions of the BOR constituent units of providing affordable higher education the BOR needs to evaluate organizational and operational changes that will maximize the efficiency and effectiveness of its Information Security Program; and

WHEREAS,   The BOR must assure that all ConnSCU constituent units maintain an Information Security Program ("ISP") that is consistent, and

WHEREAS,   It is critical that the BOR implement in a timely manner new logical and technical controls to protect the BOR confidential data and infrastructure from future breaches; therefore be it

RESOLVED,   That the BOR Chief Information Officer shall be responsible for the design, implementation, operations and compliance functions of the Information Security Program for all ConnSCU constituent units; therefore be it

RESOLVED,   That the college and university Presidents are responsible for assuring that the BOR Information Security Program inclusive of all standards, procedures, and compliance - including managerial, operational and technical controls is followed by their institution; therefore be it

RESOLVED,   That security, standards, procedures, and compliance - including managerial, operational and technical controls - shall be consistent with the National Institute of Standards (NIST), and be it

RESOLVED,   That standards and procedures for protecting information shall be consistent with state and federal laws, including but not limited to FERPA and GLBA, and be it

RESOLVED,   That all senior managers whose staff use personally identifiable information in the carrying out their institutional duties shall ensure that their staff have been provided the appropriate level of data security awareness training and are in ongoing compliance with data security standards and practices; and be it further

RESOLVED,   That all costs associated with mitigating security breaches due to a constituent's failure to comply with the BOR Information Security Program shall be the responsibility of the respective BOR constituent; and be it further

RESOLVED,   That the BOR Chief Information Officer shall annually provide the Board of Regents a report detailing the security program effectiveness and the risk the BOR is currently accepting. The report will be provided by November 15.

ConnSCU Information Security Annual BOR Report

The Information Security Program Office (ISPO) is recommending the following process for the Annual Information Security Report to the IT Subcommittee of the BOR:
- The report is broken into the following two phases:
    - Phase I – EDUCASUE Risk Assessment review using peer review – Due at November IT Subcommittee of the BOR
    - Phase II – Internal peer review of the institution security program – Due at the April IT Subcommittee of the BOR

Phase I will use the EDUCAUSE Information Security Risk Assessment template based on the following:
- The BOR will develop/create the ISPO Security Compliance Working Group (SCWG)
- The SCWG will work with each constituent unit to verify a common understanding of the questions and develop consistent answers. This may be done at meetings filling out the survey with the institution or as off-line review and discussion

Phase II will be a comprehensive review of each constituent unit information security operational practices vs. the defined BOR Information Security Program. Following are the major steps needed for the review:
- The SCWG needs to define the BOR Information Security Program based on NIST 800-53 and SANS Critical 20 controls
- The SCWG will develop an evaluation matrix and interview process to evaluate the constituent unit security operational practices**.**
- The SCWG will perform an operational review at each constituent unit
- THE SCWG will analyze the operational review against the ConnSCU Security Program and create a gap and risk analysis for the BOR IT Subcommittee

Prerequisites
- The SCWG will need to be sponsored and staffed by the colleges, universities and system office
- Membership should include:
    - BOR CISO
    - BOR Security and Policy Program Manager
    - 2-3 – university CIOs or security mangers
    - 2-4 - college IT Directors or security technicians
    - 1 – COSC CIO or security manager
- Members will need to be able to dedicate between 1 to 2 days per week until the completion of the review. The 1 to 2 days does not include time to take prerequisite training.
- Members will need to have a minimum set on Information Security Training or equivalent experience to be on the SCWG.
- The minimum sets of requirements are defined by having taken the following SANS courses or similar background.
    - MGT514: IT Security Strategic Planning, Policy and Leadership
    - SEC440: 20 Critical Security Controls: Planning, Implementing and Auditing
- Optional requirements are defined by taking the following SANS courses or similar background:
    - MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression – or – SEC401: Security Essentials Bootcamp Style
    - MGT414: SANS +S Training Program for the CISSP® Certification Exam

- The system office has purchased SANS courses to provide the necessary training for the SCWG
- If a user is wishes to take the SANS certification the university or college would need to pay for the certification. The system office can purchase the certification at the time of course enrollment and the college would reimburse the system office. The cost of certification at time of course enrollment is currently $579. It will be $599 January 1, 2014. If you do not purchase the exam at time of course enrollment the regular exam costs are $999 discounted to $849 for students who have purchased the course.
- The completion date of Phase I & II is dependent on having the SCWG defined with the group meeting the minimum requirements by September 15, 2013. If the SCWG is not operational by September 15, 2013 the completion date will need to be adjusted based on when the group is fully functional.