January 11, 2002

MEMORANDUM

TO: Mr. Sydney McKenzie, III
General Counsel, Florida Board of Education

FROM: R.E. LeMon, Vice Chancellor
Academic and Student Affairs

SUBJECT: Use of Third-Party Contractor for Graduate Candidate Identification System and Rationale for Sharing Information Protected by FERPA

The Division of Colleges and Universities has discussed the possibility of entering into a contractual relationship with the Educational Services Program at Florida State University for the purpose of housing and providing technical maintenance of the Graduate Candidate Identification System (GCID). We would like to explore with you two legal issues that have been raised by our discussions: the legal propriety of using a third-party contractor and the legal rationale for sharing information protected by the Family Educational Rights and Privacy Act (FERPA).

The Graduate Admissions Task Force originally suggested the database for the GCID. The purpose of the database is to allow Florida's public universities access to eligible students at the eleven public institutions who can be encouraged to enroll in graduate programs. The database consists of student records containing the GPA range as well as the identification number (A user of the database would not be able to access the student's identification number; this number would be used purely for the internal purposes of the database), major, race, gender, e-mail address, and local and permanent addresses and telephone numbers of students with a GPA of 2.8 and above. With the exception of the GPA, each datum can be considered to be directory information. Since the GPA is protected under FERPA, we would like to know whether such information could be provided to a third-party contractor that would maintain and house the database for the use of the eleven public universities.

When planning for the GCID began, concern about providing the GPA (which we decided to express as a range rather than as the actual GPA) led us to seek an opinion on the legal ground on which this information could be provided. Provisions in state and federal law permit disclosure of this information without permission of parents or students to " . . . school officials, including teachers within the educational institution or local educational agency,

who have been determined by such agency or institution to have legitimate educational interests" in the information contained in the records. The universities that used to comprise the State University System have determined that they have a legitimate educational interest in having access to the names and majors of at least some undergraduate students within a certain range of grade point averages, and that educational interest consists of the goal of enhancing educational opportunities to these students by contacting them and letting them know of graduate school opportunities. We would like to know if the legal provisions that allow the universities to receive and to use this information allow the Division of Colleges and Universities (DCU) to provide these services through a third-party contractor. We would also like to verify that the legal rationale for sharing this information among the state universities still applies in the context of our changed governance structure. Background information on ESP (the third-party contractor), the role it will play, and an outline of the measures it will take to ensure the security of the data is provided below.

The Educational Services Program (ESP) at Florida State University designed the Graduate Candidate Identification System at the request of and with input from DCU. The Educational Services Program has a 27-year history of providing assessment and evaluation, information and clearinghouse services, instructional design and development, and print and multimedia production. State agencies, including the Department of Education, and private agencies and businesses are among its clients. As part of the Institute of Science and Public Affairs, ESP helps to carry out the functions of the Leadership Board for Applied Research and Public Service (LBARPS), which was created by the Florida Legislature to do the following things:

1. Focus and coordinate applied research and public service activities with the Department of Education, Division of Colleges and Universities);
2. Ensure that applied research and public service activities are responsive to the needs of state and local governments, and
3. Provide accurate, timely, useful, and relevant information, when needed.

Initial funding for designing and pilot testing the database was provided by LBARPS. ESP will continue to maintain the database on their server, providing this service on a contract basis.

Security Measures

ESP will provide five key elements of security:

User Identification and Authentication

ESP designed the database to require user identification and passwords for authorized users of the database. User IDs and passwords will be stored as system control data within the server's database and used for user authentication. This should ensure that entry will be denied to unauthorized users. This control data will be stored in an encrypted form. Passwords issued to registrars for the purpose of uploading data will not enable them to search the database. A different password will be assigned to designated graduate admissions staff members that will allow them to read the database.

Security of Data Stored on ESP's Server

On an annual basis (June) university registrars will upload student records into ESP's server in a file format designed by ESP. Security of data stored on ESP's server will be provided through firewalls, appropriate in-house permissions, and data and server permissions so that unauthorized persons will not have access to the data or to information about user identifications and passwords.

Encryption of Data Communication Traffic

When files are uploaded by each university registrar and when admissions personnel read the data for recruitment purposes, the data will be protected with the use of a Secure Socket Layer (SSL). SSL allows a secure connection between the web browsers of those sending and downloading data and ESP's server. Verisign, a leading company in Internet security, will provide acceptable SSL transmission encryption capability.

Physical Security of the Server and Provision of Back-Up Procedures

ESP will provide assurance to the Division of Colleges and Universities that the server is physically secure in a controlled location to which access is restricted. ESP will also document its back-up procedures to ensure against loss of data or system or server failure.

ESP Access to Data

ESP access to the student records in the database will be limited to ESP's technical director and one assistant for administrative purposes and to enable them to provide technical assistance to universities when needed. Both will be asked to sign confidentiality agreements that will proscribe their disclosing any of the data to anyone else or making unauthorized use of the data. ESP will not have a role in the use of the student records included in the database.

The GCID has been pilot-tested and is ready to be implemented. We hope to receive a favorable response on its legal standing so it can be made available to universities to inform students of educational opportunities.

Thank you for your assistance.

REL/cjs