

**Comments of the EDUCAUSE/Internet2 Computer and Network Security Task Force on the Family Educational Rights and Privacy Act; Proposed Rule, *Federal Register*, Vol. 73, No. 57, U.S. Department of Education, Office of Planning, Evaluation and Policy Development
Docket ID ED-2008-OPEPD-0002**

May 8, 2008

The EDUCAUSE/Internet2 Computer and Network Security Task Force supports the ongoing efforts of the Family Policy Compliance Office in the U.S. Department of Education to promote the privacy of student education records. While we share the concern that underlies the department's "Recommendations for Safeguarding Education Records" (*Federal Register*, vol. 73, no. 57, p. 15598), it is not clear to us why this discussion was included in the notice about the proposed rules since information security is not addressed in the proposed regulations. The inclusion of recommended safeguards causes considerable confusion about the department's intentions and future plans.

Additionally, the reference to resources from the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) raises questions about the department's position on the appropriateness of federal standards mandated by the Federal Information Security Management Act (FISMA), the federal law on which NIST and OMB guidance is based. Although the comments acknowledge that these documents are directed toward federal agencies and are provided as informational resources only, the singling out of federal government guidance documents at the exclusion of other sources developed by private sector groups and standards organizations is disconcerting. For example, many colleges and universities are adopting international standards such as the ISO 27002 ("Information technology. Security techniques. Code of practice for information security management").

Significant resources are also available from the EDUCAUSE/Internet2 Security Task Force. The task force was created in 2000 "to improve information security and privacy across the higher education sector by actively developing and promoting effective practices and solutions for the protection of critical IT assets and infrastructures." (<http://www.educause.edu/AboutTheTaskForce/1202>). The task force has created several useful resources and tools that we urge you incorporate into your recommendations if you decide to continue to include them:

Confidential Data Handling Blueprint

<http://www.educause.edu/security/datahandling>

Data Incident Notification Toolkit

<http://www.educause.edu/security/incidentnotification>

Effective IT Security Practices Guide

<http://www.educause.edu/security/guide>

Information Security Governance Self-Assessment Tool for Higher Education

<http://www.educause.edu/ir/library/pdf/SEC0421.pdf>

We would be happy to discuss these efforts in more detail with the department. We urge the department to carefully consider the implications of proposing recommendations or rules for information security, given the breadth of resources available and the complex nature of existing compliance requirements for colleges and universities.