



Cybersecurity

Background

Security has always been a component of system management. Integrity of data has been a concern since the first students broke into a system and successfully changed their grades. But interconnectivity has moved information technology issues from the class room and machine room to the board room. At the national level, with the growing dependence on the Internet and the increased threat of terrorism, IT security issues have ascended right into the White House.

As the owners and caretakers of powerful computing resources, the higher education community is recognized as a major component of our national cyber infrastructure. EDUCAUSE played a role in the development of the *National Strategy to Secure Cyberspace*. In April 2002, we joined with the American Council on Education (ACE) along with the other members of the Higher Education Information Technology Alliance (HEITA) in ratifying the *Framework for Action*. It was presented to Richard Clarke, then special advisor to the president for cyberspace security, in October 2002.

The *National Strategy* was released by President Bush in February 2003. Within the strategy, higher education recognizes the need to improve the security of their computer networks both for its own benefit, as well as to be a “good citizen.” A *Framework for Action* was developed to signify the priority status that must be given to this issue. The framework sets forth the following goals:

- Make IT security a priority in higher education
- Maximize the use of existing security tools including policies
- Design improved security into new systems prior to deployment
- Increase collaboration between academic institutions, the private sector, and government
- Become an example of how to successfully deploy security in a complex and dynamic environment

At the federal level, with the release of the *National Strategy*, infrastructure security will gradually move from its strategy phase into implementation planning and management. The U.S. Department of Homeland Security (DHS), at the center of that transition, is set to house the “fusion” center where cybersecurity information will be gathered, analyzed, and disseminated. The issues generally break down into three main categories:

- **How to get the private sector to voluntarily secure its own systems:** At what point will mandates be necessary to protect the national infrastructure? What federal action is warranted if a private facility does not follow good security procedures? What education efforts are needed?
- **How to gather, coordinate and use the necessary information:** DHS will be responsible for domestic cybersecurity information, but what is the best way to promote a two-way flow of information?
- **How to effectively use resources:** How can the federal government, academia, the private sector, the Department of Defense, and other areas most effectively use their resources to encourage research into new security technology?

Significance for EDUCAUSE Members

Establishing a secure environment that allows for the maximum level of personal freedom is a worthy goal. How successfully we secure our own systems, share vital information, and participate in the national

dialogue will largely determine what role the federal government will need to take in the future. Ideas for improving system security need to be developed and shared with academic researchers, and grant proposals need to be targeted to fill this vital need. Whether the Federal Government becomes the facilitator or the policeman largely depends on how this work progresses in the coming months and years.

Current EDUCAUSE Position

With their unique social position between the commercial and government sectors, institutions of higher learning have the opportunity to show how security can be accomplished in a diverse, complex, and dynamic environment while still maintaining essential freedoms. Their leadership can provide a basis for improving the national infrastructure and preclude the need for “top-down,” cumbersome, Federal regulation. At the very minimum, the EDUCAUSE community must play an active role in the dialogue as these issues are examined and policies established at the National level.

Leading the Cybersecurity Effort at the Federal Level

Department of Homeland Security Information Analysis and Infrastructure Protection Directorate, <http://www.dhs.gov/dhspublic/theme_home6.jsp>.

Federal Bureau of Investigation InfraGard Program, <<http://www.infragard.net/>>.

Congressional Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research and Development, <<http://hsc.house.gov/content.cfm?id=18>>.

Resources

EDUCAUSE resources on the *National Strategy to Secure Cyberspace*, <http://www.educause.edu/Browse/645&PARENT_ID=654>.

EDUCAUSE/Internet2 Computer and Network Security Task Force, <<http://www.educause.edu/security/>>.