TO: Polley McClure
FROM: Tracy Mitrano
RE: Impact Statement for University Policy on Authorization and Authentication
DATE: March 7, 2003

According to University Policy 4.1, Formulation and Issuance of University Policies, I am writing to request that you, as Responsible Executive Officer, present to the Executive Policy Review Group for general approval the attached impact statement for a proposed university policy on network identification, authentication and authorization.

I. BACKGROUND

Since the advent of computer systems, Cornell has attempted to control access to its electronic resources to facilitate its business and educational mission through a variety of authentication and authorization mechanisms and identifiers. Such an incremental approach has inadequately served Cornell’s overall authentication and authorization requirements and has failed to achieve a comprehensive approach that can accommodate new services or technologies.

This policy creates a comprehensive strategy for controlling electronic access and coordinating deployment of university authentication and authorization mechanisms.

II. CONTROVERSIAL ISSUES

This proposed policy anticipates the following issues, some of which may be controversial and/or may imply unfunded mandates and yet to be developed technologies:

- Units may have practices already in place which will conflict with this policy;
- Independent of existing practices, units may want to assume control over authentication procedures in a manner which conflicts with this policy or any comprehensive approach to a university-wide strategy;
- Units may expect CIT to provide unique authorization for services rather than establish their own policies, procedures for their services.

The efficiency of providing a comprehensive strategy for authentication and authorization services for the university should far outweigh the inefficiencies associated with current practices or projected future dispersion of distributed services that have been deployed inconsistently.

III. GOALS

To establish a comprehensive strategy and implementation plan for authentication and authorization services consistently deployed throughout the university.
In situations where combined principals are greater than one hundred (100), Cornell University will assign unique electronic identifier(s) to anyone who has a business or education need to access a service that requires authentication. Authorization for services provided by the university depends on the individual’s relationship, or relationships, to the university and the operational policies associated with that role. The CIT Identity Management Program, in consultation with the IT Security Program, will establish the framework for Cornell’s authentication and authorization strategies and convene a task force, chaired by these offices and including broad representation from the Cornell community, to develop the operational policies commensurate with that goal.

The university must control access to its electronic, physical, and financial resources to facilitate its operations and further its educational missions. Failure to control access appropriately may have deleterious financial and legal consequences or may adversely affect the institution’s reputation.

- Endowed-Ithaca and Contract Colleges of the University (Excluding the Joan and Sanford I. Weill Medical College)

- All Members of the University Community

*The Policy Office web pages house the most current versions of all standardized university policies, at http://www.univco.cornell.edu/policy/home.html