Minutes*

Senate Research Committee
Monday, May 9, 2005
1:15 - 3:00
238A Morrill Hall

Present: Gary Balas (chair), Mark Ascerno, Dianne Bartels, Richard Bianco, Christopher Cramer, Dan Dahlberg, Sharon Danes, Kathy Ensrud, Genevieve Escure, Steven Gantt, Michael Hughey, Paul Johnson, James Luby, James Orf, Mark Paller, Mira Reinberg, Maria Sera, Charles Spetland, George Trachte, Barbara VanDrasek, Jean Witson

Absent: Victor Bloomfield, James Cotter, Robin Dittman, Timothy Mulcahy, Thomas Schumacher, Virginia Seybold, Michael Volna

Guests: Associate Vice President Steve Cawley, Ken Hanna (Office of Information Technology)

Other: Melinda Sewell (Office of the Vice President for Research)

[In these minutes: (1) individual conflict of interest policy; (2) strategic planning recommendations; (3) openness in research policy; (4) Department of Homeland Security research; (5) data security; (6) resolution]

1. Individual Conflict of Interest Policy

Professor Balas convened the meeting at 1:15 and turned to Assistant Vice President Bianco for a discussion of the Individual Conflict of Interest Policy. Mr. Bianco in turn introduced Dr. Melinda Sewell, the expert on the policy.

The earlier policy dealt only with research, Mr. Bianco said. It is being updated as part of the routine review of regental policies and was in the queue. There are no significant changes to the policy, he said; apart from elimination of a public-private partnership committee (which was never formed), the changes are primarily organizational. The University does have a functioning individual-conflict-of-interest review system, with two committees that deal with hundreds of disclosures and management plans.

Professor Cramer observed that the policy says one must file a REPA (Report of External Professional Activities) when submitting a grant, but later in the policy it says one must have one on file. Mr. Bianco said that there must be one submitted each year but also a new one if there is a new potential conflict of interest.

Dr. Paller asked if no broader or controversial topics arose during the review of the policy. Mr. Bianco said not; this is a very good policy. Committee members posed several questions about specifics of the policy, which Mr. Bianco answered to their satisfaction. Among other points he made were these: contributions covered by the policy could include a gift to the Foundation in support of research activities

* These minutes reflect discussion and debate at a meeting of a committee of the University of Minnesota Senate or Twin Cities Campus Assembly; none of the comments, conclusions, or actions reported in these minutes represents the views of, nor are they binding on, the Senate or Assembly, the Administration, or the Board of Regents.

that might carry a promise or expectation; the $10,000 threshold does not apply to funds invested in retirement accounts; in general the policy does not cover students (except if they are explicitly listed on a grant as a primary investigator); and the most frequent conflicts of interest arise when faculty license a technology to an outside company, when companies sponsor specific research, and when faculty serve as a consultant to a company that is also a research sponsor for that faculty member. Less than $10,000 from a company (e.g., royalties) are exempt; if someone receives more than $10,000 from a successful textbook, it is unlikely there would be a conflict because textbook companies typically do not sponsor other activities at the University. Assigning one's own text to a class is covered by a different policy. Mr. Bianco agreed that it is unclear when one must file a REPA with respect to royalties. What triggers the University's interest is not whether there is a $10 or $10,000 interest but whether or not there is a potential conflict. For practical purposes, there needs to be a triggering amount, hence the $10,000 figure.

If an investigator running a clinical trial gets a donation from one of the trial subjects, is that a conflict of interest, Ms. Witson asked? Mr. Bianco responded that it is not. It is only a conflict if the money comes from the sponsor of the research.

Professor Balas inquired about the REPA versus the ROC (Request for Consultant or Outside Service Agreement). They are entirely separate, Mr. Bianco said; one must file another REPA if there is a new potential conflict of interest; the ROC is only a time-management tool that may or may not include a conflict of interest.

Mr. Bianco also reported that the Institutional Conflict of Interest Policy has gone to the Board of Regents, after 18 months of work on it.

Professor Balas thanked Mr. Bianco for his report.

2. Strategic Planning Recommendations

Professor Balas reported that the President's recommendations to the Regents are very similar to the recommendations contained in the task force reports he received from the Provost. This Committee, he recalled, asked for creation of a task force on the research infrastructure; the actual recommendation closest to that request is a call for a task force to look at issues of interdisciplinary work and big science. It is not requested to look at core issues of research. [Note: in a subsequent meeting with the Faculty Consultative Committee, the President said he would support the task force looking at the issues identified by the Senate Research Committee.] The President also recommends a task force on integrating the biological sciences and engineering, but otherwise there is nothing about research. In response to a question from Professor Johnson, Professor Balas said the President's recommendations were silent on funding the Graduate School.

Dr. Paller commented that the strategic planning that has been taking place in the Academic Health Center is very detailed; people who have been commenting on the task force recommendations seem not to have been aware of that effort.

Professor Balas noted the President's recommendation to merge COAFES and the College of Natural Resources; is that positive, he asked? Professor Ascerno said that COAFES views it as positive. There are a lot of long-standing relationships between the two units on both agricultural and environmental issues. COAFES has about 220 faculty; CNR has about 45-50. Professor Orf said the two units were together at one point; this puts back together what was taken apart. The recommendation also

calls for examining facilities around the state, Professor Luby observed; some are associated with COAFES and some with CNR. It is not clear what will come out of this process, but a number of the facilities are involved in research while some are more involved in education and outreach.

Professor Balas said he hoped that the task force on reconfiguring science and engineering is broader than just the Medical School. Dr. Paller said that the College of Biological Sciences and the Medical School already share a number of departments; what happens affects more than those departments, but faculty are in jointly-managed departments and have largely been operating successfully.

Professor Balas, in response to a question from Professor Bartels, said he would be glad to write a note to the President asking about the role of the Vice President for Research and the scope of the charge to any task force appointed to deal with research issues.

3. Openness in Research Policy

Professor Balas turned next to the Openness in Research policy (formerly called the Research Secrecy policy). The subcommittee dealing with the policy has scheduled another meeting to deal with issues that this Committee raised; its recommendations will be brought back in the fall.

Professor Balas also reported that he also went to a meeting of the Committee on Social Concerns; its members were most interested in contracts in place to evaluate drugs. Someone in the Academic Health Center, for example, could get a contract to evaluate drugs as a cure and the research could be inconclusive or the drug demonstrated to be unsuccessful—and the research never published. His understanding, he said, is that contracts for hire are not covered by the policy because they are not research, they are evaluation. Dr. Paller said that it is possible to provide a service such as product evaluation (which counts as external sales—which must meet a strict definition). For example, the University may have a machine with excess capacity to provide assays; the University may use it for commercial entities not involved in any University research at all. It would send the results to the company with no right to publish anything. But if the University discovered something with respect to use of the machine, it would retain full rights over the discovery. Anything that requires analysis is research and must go through Sponsored Projects Administration; SPA will not approve any contract with restrictions on the University's right to publish. It is not a problem to do research that is temporarily blockaded in order to provide time to protect intellectual property, and the University does give companies the right to review manuscripts in order to be sure they are not revealing proprietary information. But the University's policy is very protective of the faculty's rights, Dr. Paller assured the Committee.

Mr. Bianco agreed with Dr. Paller. He said he evaluates devices to be sure they are safe. Those are not external sales and the University reserves the right to publish.

These are examples like testing toasters, Professor Balas commented. The Social Concerns Committee was mainly concerned about other topics.

4. Department of Homeland Security Research

Dr. Paller said he wished to bring up an issue in order to obtain Committee members' views about it. The Department of Homeland Security (DHS), new to the business of giving research grants, is

interested in changing the way it deals with research it funds. This is an idea, not policy, he cautioned, and is simply on the table for discussion.

DHS is concerned that in the course of doing research at the University, faculty could discover something with security implications. If it CLEARLY has security implications, the federal government can march in and declare the research classified. DHS has proposed a peer review process, centers of excellence, to look at their own publications and allow a voluntary decision not to publish. How does the Committee feel about that, he asked? It could be a slippery slope, he observed, and DHS could be more demanding the next time a grant came up for renewal if it dealt with issues with potential security implications. It might turn down funding if articles were being published.

This is all a slippery slope, Ms. Witson said. A lot of people are involved in research that DHS could see as potentially of use to terrorists. Dr. Paller said that so far the University's Center of Excellence and others have been asked about the subject by DHS. In that context he's asking faculty to think about it. This is all speculation, he emphasized, but the more discussion the University has, the easier it will be to respond to any proposed rule. At some point the University would need to say "no." What if a grant recipient accepts restrictions but the Committee believes that the self-evaluation impinges on research openness? Professor Dahlberg said one could always ask people to look at one's research, and if a committee exists, one can voluntarily have the committee look at the research. But that will soon become a requirement, he predicted. This would only affect people receiving funding, Dr. Paller said, and everyone would know it is part of a grant if one takes the money.

Would it be required that a PI follow the committee recommendations, Professor Orf asked? As they have discussed the idea, Dr. Paller said, there would be no requirement for a researcher to follow the recommendation. If it were required, then someone could be stopped from doing research. If it is voluntary, a majority of the committee could persuade. It would preserve academic freedom to not require that committee recommendations be followed.

Professor Balas said he worried about side agreements between the researcher and the agency. The researcher would know he or she could publish but would promise not to. The point is not to stop research, Dr. Paller said, but to check for sensitive details. What he has been talking about is the faculty themselves doing the reviewing. Peer pressure can be stronger that the government, Professor Balas maintained; if one is out of step, people know who not to invite. It is also hard for any faculty member to know what might be on the mind of DHS, Professor Bartels commented.

Dr. Paller cited an example. Perhaps there is a chlorine plant in New Jersey that is a potential terrorist target. A question is whether one should publish an article modeling the effect of a terrorist attack on the plant. Is there anything wrong with peers having that conversation? There is nothing wrong with investigators doing that kind of analysis, Ms. Witson said, but she has a problem with putting the requirement into a contract. Professor Escure questioned whether federal oversight might inhibit the sharing of ideas at international conferences.

5. Data Security

Professor Balas next welcomed Associate Vice President Cawley and Mr. Hanna to the meeting to discuss data security.

University policy is to protect data that is legally and contractually private, Mr. Cawley explained, and the data must meet the standards set by the law. The requirements, however, seem to be ratcheted up each year, HIPPA, for example, caused an increase in security requirements, as do other federal regulations. The University has taken the position that it should not have different standards for different localities—it should have the same level of assurance about data across the campus.

One question from this Committee was what researchers are to do with existing data and what help they can get. The University is a decentralized and complex organization, Mr. Cawley commented. In the Academic Health Center, for example, all computers must meet the University's Securing Private Data Standard; since private data can move easily between computers, all must meet the standard. Support and recommendations elsewhere on the Twin Cities campus vary by college; his office is engaged in discussion with a number of units, he reported.

One thing they are discussing is the University providing to all researchers central data storage with a secure backup. If they can provide central file space, the process would be more manageable for researchers and they would only need to worry about their desktops. The University has requested funding to provide this service, which would allow building a storage service available to every researcher.

A recent change is operating requirements: having competent security staff to manage computers. That is as important as setting the dials correctly, Mr. Cawley said. The only time that happens now is when someone has "hacked" a server, at which point a machine is locked and the unit assesses its information technology management.

Ms. Witson, noting that she is involved in clinical trials, said that all their computers have controlled access. Their question is about server security: if their computers are taken care of as they should be, are the data as secure on their hard drives as they would be on a server? Mr. Hanna said that laptops constitute the highest risk because they are so easily stolen; one should PLAN on them being stolen in terms of thinking about data security. Data should be stored encrypted or on a server. Desktop computers are also high-risk, which is why they came up with tools to secure them. For best security, they recommend using a server and keeping private data/information off laptops.

Professor Ascerno asked if it can be made easier to work from a laptop to a server. There is a logistical problem if one works remotely. There are a couple of choices, Mr. Hanna said. One is to try not to work remotely, or get the data downloaded but encrypted (the theft risk remains high). They are not good choices, he agreed, and the risks are high. And the press is paying attention to incidents of data release, he added.

Professor Balas asked about the number of research contracts that include working with private data. Mr. Hanna said he has not run across any but there will be more.

Professor Escure asked about getting access to email from abroad. Mr. Cawley said that for the central University email servers it can be done from any mail browser, and even if one is in an unsecured environment (e.g., wireless), the SSL connection to the University webmail automatically encrypts email so no one can snoop. Another option is to use secure SSL setting in the email client (Outlook, Eudora, etc.). The third option is to use a Virtual Private Network client, which is software that is free that needs to be downloaded and installed on the computer. Once the VPN program is started, it encrypts the network traffic such as emails or web pages. One loses security in an internet café, Professor Escure

suggested. Mr. Hanna agreed that even if a secure connection such SSL or VPN is used, if there is a keylogger all bets are off. The keystrokes could give away the passwords and other information typed. Mr. Cawley said that the Office of the General Counsel, for example, assumes most of its email is confidential and its staff cannot use internet café computers—or hotel computers.

Professor Cramer asked about the quality of the Macintosh security program. It is very good, Mr. Hanna said. Microsoft also has good security, Mr. Cawley said, but if one loses the key, one loses the data. He said they are struggling with the problem of laptops. There is a lot of mobile computing taking place, and they do not want to ban an easy way to work, but if one wants to work on a laptop, it is important not to lose the key.

The Committee discussed the support provided by the University for operating systems (they support the latest systems for Mac, PCs, and Linux, and would like to drop OS9, Windows 98, etc., because later systems are more secure and staff doesn't have to work with so many systems). Macs will not go away, Mr. Cawley assured Committee members.

Professor Balas commented that faculty will respond to incentives, such as if money were provided centrally for people to get their computers updated and hard disks cleaned. Why not encourage faculty and staff in more creative ways? Rather than adopt policies? They are trying, Mr. Cawley said. University Computing Services will clean hard disks and eliminate data as well as refurbish or recycle computers. They have not gone to offering carrots, which might be a good idea. They could do the same with operating system upgrades. They need to be proactive to get faculty to buy in for new data and security standards, Professor Balas told Mr. Cawley.

They have not been able to get a deal from Microsoft for student computers, Mr. Cawley said; students are the biggest liability. They want to be able to offer operating systems to students for free. Mr. Hanna pointed out that the Symantec anti-virus program already is free and includes one copy for home computers. Committee members said they cannot figure out how to get it set up; Professor Escure asked if there was any reason the University could not install the anti-virus software on home computers as well. Except for financial constraints, it may be possible, Mr. Cawley said. It would be complicated to support the home computers (e.g., children can play havoc with security). There is also the problem of the University maintaining someone's personal property at home, Mr. Hanna added. It is an issue that needs revisiting, Mr. Cawley said, because it is an area of significant vulnerability.

Professor Dahlberg agreed that security is a big concern for all University faculty and students, and one can see the issue with respect to things like personnel files. But he said he has no virus-protection software, encrypts certain things, and has never had a problem. (Note added after the meeting: he uses pine on a UNIX mainframe for all email and relies on the mainframe software, more regularly updated than an individual would, to find viruses.) Why would anyone break into his computer? It is a loaded gun, Mr. Hanna replied: it can be used by others for bad purposes (e.g., sending spam through it). Since he is in the University community, which has passwords, one can call up personal information. People do not recognize what can happen if someone else puts something on one's machine, such as porn or copyrighted materials (called warez in the hacker community), which could result in lots of potential problems and hassles. Additionally, some viruses and Trojans have keyloggers, so the risk is high. There are a lot of reasons not to be blasé about security, one of which is being careful for others at the University.

It is not that faculty generally are resistant to increased security, Professor Ascerno said, but they lack the knowledge about why it is important and the technical expertise to use it. Right now the education and technical support is passive; the Office of Information Technology needs to be more aggressive. Mr. Hanna agreed. Mr. Cawley said that his office and the Academic Health Center have partnered to create online course modules for security. They are also starting, in June, a server-administration course, Mr. Hanna reported, that will be free.

Can administrators snoop on one's email, Professor Escure asked? Mr. Cawley said they always turn over to the General Counsel any request to read email. The employer does have certain rights, but in practical terms the University tries to respect privacy as much as it can. He said the Committee should address these questions to Tracy Smith in the General Counsel's office. From a technical standpoint, Dr. Van Drasek said, it is absolutely clear that administrators can read email. The University's policy, however, directs administrators not to do so unless they are troubleshooting a problem or working with the Office of the General Counsel, Mr. Cawley said. Mr. Hanna said they consult with the General Counsel any time there is a question related to private data or when someone insists that someone else is reading their email.

Professor Ascerno observed that the University has systems that screen out email before one even sees it, and he has lost some emails because of the screens. It is possible, however, to lift the screen for senders if one wishes. He looks at the emails that have been screened each week—it is a very long list. In most cases, one cannot tell what the subject of the email is.

Professor Balas thanked Messrs. Cawley and Hanna for joining the meeting.

6. Resolution

Professor Cramer introduced and moved the Committee adopt the following resolution:

> Whereas, Professor Gary Balas has served actively and faithfully for three years as chair of the Senate Research Committee, and for four years as one of the most conscientious members of the Committee, and
>
> Whereas, the members of the Research Committee have appreciated Professor Balas's industry, good humor, and devotion to the advancement of the best interests of the University of Minnesota and its research enterprise,
>
> Therefore Be It Resolved that the members of the Senate Research Committee thank Professor Balas for his service as chair of the Committee and wish him the best as he leaves this Committee and begins his service on the Faculty Consultative Committee, where, we are confident, he will continue to be a strong voice for the interests of the faculty, and for research.

The Committee voted unanimously in favor of the resolution.

Professor Balas thanked his colleagues for the kind words and adjourned the meeting at 2:45.

-- Gary Engstrand