NIH Seeks Reduction in "Indirect Costs"

Dispute about reimbursement for overhead is creating tension between university administrators and academic researchers

A long-simmering dispute between academic scientists and university administrators over funds for the "indirect costs" of research moved a bit off dead center last month when administrators conceded that a steep rise in the cost of overhead, including energy, libraries, and "departmental administration" is something of a problem.

When the National Institutes of Health (NIH) awards a grant, both researchers and institutions stand to benefit. The principal investigator receives funds for the "direct costs" of the research; the institution is reimbursed in full for the indirect costs of carrying it out. It is a payment system designed to please everyone that has, instead, become the focus of an acrimonious debate about whether ever-increasing indirect costs are claiming an unfair proportion of the NIH research dollar. NIH director James B. Wyngaarden, who has confronted the issue head-on, would like to see some restraints put on indirect cost reimbursement which has achieved something of the status of an uncontrollable entitlement program in recent years.

According to a policy statement by Wyngaarden, "Since 1966, when [the government] made full reimbursement of indirect costs a central element of its grants policy, indirect costs have been consuming an ever-greater fraction of the funds available for grants, accounting for 30% of the total in FY 1982." Wyngaarden notes that in terms of constant dollars for FY 1970, the amounts awarded for investigator-initiated basic research grants has remained "essentially level from FY 1970 through FY 1982, in spite of the increased complexity of research. Indirect costs during that same 13 year period rose more than 50%."

Grant proposals, which are submitted to peer review for scientific merit, are also scrutinized on a fiscal basis. It is not uncommon for a peer review committee to recommend approval at a funding level 10 percent or more below what an investigator asks for. By contrast, indirect costs are reimbursed according to strict accounting procedures that automatically accept claims for "allowable" items under provisions of Circular-A21 of the Office of Management and Budget (OMB). There is no peer review, although claims must be approved by federal auditors. Furthermore, it frequently happens that indirect costs are adjusted upwards during the life of a grant, whereas direct costs are clearly fixed. "Indirect costs," says Wyngaarden, "have had preferrect access to grant support dollars." He thinks that indirect costs should be subject to "new restraints."

A first step, he suggests, would be to rescind the current policy that allows upward adjustments of the indirect cost rate to accommodate cost increases during the life of a grant.

In general, university administrators, who argue that indirect costs are every bit as "real" as direct costs, disagree with Wyngaarden's position. Last February, Wyngaarden convened a meeting of persons representing both sides of the issue to help prepare a report on indirect costs for the House Committee on Appropriations. A draft report containing several approaches to cost-containment was submitted as a working paper. But the essence of the dispute became clear even before the meeting was held. The day before the conference, officials from the Association of American Universities, the National Association of State Universities & Land-Grant Colleges, and the American Council on Education, jointly representing university administrators, wrote Wyngaarden to say the draft was not an "acceptable" basis for discussion. Citing its "inference" that indirect costs are not true parts of grants and that such costs have risen "disproportionately," the university representatives said, "It is precisely the truth of those two propositions that is at issue."

By most accounts, the February meeting resolved little if anything at all. In a summary of the discussion, the university representatives turned the question around from one of rising indirect costs to one of NIH research support in general. "We do not believe that indirect costs are rising disproportionately," they said. "On the contrary, we believe that monies for direct costs are not rising fast enough to meet the needs of inflation." (Were general research revenues to rise as much as NIH officials might wish, they likely would not argue with this proposition.)

Subsequent meetings have been somewhat more conciliatory although the issue remains contentious. In late June, NIH officials met with representatives of various groups, including the Association of American Medical Colleges and the American Federation for Clinical Research, which tend to see the issue more from the researchers' point of view. Then, the idea of temporarily passing the whole matter off for further study gained support when it was tentatively agreed that Presidential science adviser George A. Keyworth, Jr., be asked to approach the National Academy of Sciences (NAS) about doing a study of indirect costs, including the reasons for their substantial increase during the past decade.

In July, both sides of academe met in Washington again—this time without NIH officials—to find mutual ground. A summary statement of that meeting, written by Stanford University president Donald Kennedy and Lattie Coor, president of the University of Vermont, endorsed the NAS study idea but also called on NIH to suspend its indirect cost containment efforts until such a study is complete. One effect of such a study would be to review the question of indirect costs government-wide, rather than just as it pertains to NIH.

The Kennedy-Coor letter attacked NIH's various cost-containment approaches, saying "The NIH proposals to reduce reimbursement of those costs selectively, by whatever mechanism, will directly damage the research effort as a whole." But they went on to say, "We recognize, however, that the proportional rise in indirect costs poses long range problems for that effort." The latter sentence has been interpreted as a major concession by university administrators, particularly because they also said, ". . . we agreed that indirect costs as a category are particularly important targets for economy in our institutions."

The July meeting also focused attention on the strain these arguments over indirect costs have created within universities. "Naturally, faculty members complain that their administrations are often confusing or opaque in their explanations [of what legitimate indirect costs are]; and conversely, administrators

sometimes feel that their faculty constituents are refactory to explanation," Kennedy and Coor said. The fact that both sides acknowledged the problem and agreed to try to have a useful "dialog" is, in itself, considered a mark of progress in an argument that must ultimately be settled by Congress, which has not gone along with recent attempts to reduce funds for indirect cost reimbursement. The issue is likely to come up again when the next NIH budget is prepared. It is also the subject of a report soon to be released by the General Accounting Office.—**BARBARA J. CULLITON**

Computer Break-Ins Fan Security Fears

But experts say computers containing classified material are invulnerable and that others can be made more secure

In early August, it was reported that a group of young people in Milwaukee broke into a computer at Los Alamos National Laboratory. The break-in attracted an extraordinary amount of publicity, in part stimulated by the popular movie *War Games*, in which a teenager is depicted breaking into a Defense Department computer and almost precipitating World War III.

Shortly after the Los Alamos break-in was reported, an alarming entry into a computer at Memorial Sloan-Kettering Cancer Center in New York hit the headlines. In this incident, a computer hack, who apparently is a member of the Milwaukee group, used a $1200 Apple computer to gain access to patient records.

These incidents have raised concerns that classified data and other sensitive information stored in computers might be readily available to anyone with a terminal, including foreign agents or people engaged in industrial espionage. Computer security experts maintain, however, that computers containing highly classified information are virtually invulnerable because they are not linked to any outside system. It is therefore impossible for anyone to dial into them. Moreover, experts say that even computers that are linked to outside networks can be made more secure so that break-ins can be quickly detected.

The Los Alamos computer was being used to develop an electronic mail system and it contained no sensitive information. Therefore it was not heavily protected against break-ins. Such a procedure makes excellent sense, says Robert Courtney, a computer crime consultant living in New York. "It would be dead wrong to secure that which is not worth securing. The idea is to try and make systems as usable as you can," Courtney explains. The key point about the Los Alamos and Sloan-Kettering break-ins are that the security controls on the computers there were not at all like those on computers containing classified information. Yet even with those relatively lax controls, the Milwaukee youths were traced and identified.

The controls on computers that contain classified information cannot be broken at all, experts say. "I do not know any way even remotely possible of getting into those computers without a breach of trust," says Robert Morris, a computer security expert at Bell Laboratories in Whippany, New Jersey, who is often asked to try to break into computers to test their vulnerability.

Computers containing classified data are isolated from the outside world, so that no one—not even people with clearances to work on the computers—can dial a phone number from their home or other insecure area and log into them. The Milwaukee group dialed into networks that connect insecure computers and then logged into computers in the network. The Los Alamos and Sloan-Kettering computers are connected to Telenet, a commercial network.

The Cray computer at Sandia National Laboratory is typical of those that contain classified information. No unauthorized persons are allowed into the heavily guarded facility where scientists primarily work on the engineering of nuclear weapons. The Cray is "Tempest-certified" by the National Security Agency (NSA), meaning that no electromagnetic radiation can be detected outside the computer room. The NSA worries that if radiation escapes, it could be "read" by special equipment to reveal what information the computer is processing. Every terminal for the Cray is also Tempest-certified.

The Cray computer is linked to a computer at Los Alamos that also contains classified information. But the data that flow between the two computers cannot be read by tapping the link between them. Those data are encrypted with codes supplied by the NSA. The keys for decrypting at either end are delivered by courier. "I don't expect to see one of those [codes] broken during my career," says Gus Simmons, the manager of Sandia's mathematics department.

Many computers containing classified information are not linked to other computers at all. But the Department of Defense and the intelligence agencies do have their own private networks to connect secure computers. The DOD network is called World Wide Military Command and Control System, or WWMCCS, and the network used by the NSA and the Central Intelligence Agency is called Community On-Line Intelligence Network System, or COINS. Like those at Sandia and Los Alamos, computers in these networks cannot be reached by dialing outside telephones. They can only be used in "secure areas" that are Tempest-certified and the data flowing between the computers are encrypted. "I'm a skeptic, not a believer, but every thing I've seen of those systems makes me feel secure," Morris says.

But security comes at a price: the computers are fairly cumbersome to use. Mostly because of the inconvenience of working in the special rooms at Sandia containing the Cray terminals, members of Simmons' group tend not to use the Cray unless it is absolutely necessary. Currently, only 3 of the 24 group members are using the Cray, Simmons says.

Another difficulty with these computers is that only people with the highest security clearances can use them. For example, if a computer contains both top secret, secret, and confidential information, only people with top secret clearances would be allowed to use it because it is impossible, in most cases, to prevent people from getting at any files they want once they have access to a computer.

This stratification of computers is expensive and awkward and the DOD would very much like to see computers designed so that they can effectively separate different classes of users. One computer, the Multex, built by Honeywell, can apparently keep one group of