late strategies for protecting them.

'Born vulnerable.' NSDD 145 was the subject of a Congressional hearing before the House Government Operations Committee on 27 June, when Robert L. Brotzman, director of the Pentagon's Computer Security Center at Fort Meade, Maryland, argued that computer systems are largely "born vulnerable." The widespread lack of protection for both computers and computer telecommunications networks, said Brotzman, means that Soviet bloc agents, terrorists, mischievous hackers and anyone who simply bears a grudge against society could "cause great harm with very little effort or expense." Eventually, whatever policies and guidelines are adopted will apply equally to academic, industrial, commercial and private telecommunications and computer operations.

Testifying for the Institute of Electrical and Electronics Engineers, John M. Richardson of the National Academy of Sciences's National Research Council agreed with the need to protect the transmission and processing of classified and sensitive, though unclassified, government information. This is already covered by laws—the latest being the four-year extension of the Export Administration Act, signed by President Reagan on 12 July. But Richardson questioned how far NSDD 145 would extend to both academic and commercial research and information, which, in their most advanced forms, are almost always committed to computers. If the directive reached so far that it led to "regulation, restraint and monitoring," said Richardson, "we see a real possibility of collision with constitutional principles of individual privacy and freedom of speech." In its worry that the zeal of the DOD and NSA may inhibit or limit the open dissemination of unclassified scientific and technical information, IEEE has been joined by the Aerospace Industries Association and the Electronic Industries Association.

'Achilles heel.' While the specter of surreptitious access to computers and purloined misuse of telecommunications has haunted the government for more than three decades, the situation is compounded now by more powerful machines and modems. Some supercomputers are used for designing nuclear weapons and translating coded messages. For those purposes, they have been in the hands of experts with top security clearances. With the advent of supercomputers on campuses and in commercial enterprises, however, the government's intelligence community views widened access, says Senator William S. Cohen, a Republican from Maine, as "the Achilles heel" to "trespass upon private or privileged information." The concern is that certain foreign nationals (and, possibly, terrorists) will gain access to supercomputers and their networks to execute codes that might threaten or disrupt US security or obtain data on scientific research or military technology that are classified or critical. In addition, there is a fear that potential adversaries will run research programs they cannot perform on less powerful machines at home and that they will learn how to reconstruct the system architecture and recreate its software.

Last June, as the first organizations caught between the rock of national security and the hard place of academic freedom, the supercomputer centers were faced with the immediate problem of negotiating their contracts with NSF. Presented with the proviso on Soviet and Chinese researchers, university administrators refused to sign. When push came to shove, though, it was NSF that backed down, finessing the issue by including a statement to the effect that each center would abide by the policy eventually adopted by the government, whatever that may be. This was acceptable to both the University of California at San Diego, which will run its Cray X-MP at nearby GA Technologies, and the von Neumann Center, which will operate a Cyber 205. The von Neumann Center reserves the option of withdrawing if the policy infringes on academic freedom. But the University of Illinois, where an X-MP is to be installed, and Cornell, which will have an experimental center with an IBM 3084 QX mainframe and a number of FPS 164 and 264 array processors, objected to the reworked clause. After an exchange of letters and visits, NSF dropped the requirement for Illinois and Cornell. The agency's general counsel, Charles H. Herz, observed: "Of course, if there is a national policy, signed by the President, we would have to enforce it."

In the event, the centers would have to evaluate their academic research interests against the government's supercomputer policy. According to Arthur Kusinski, Herz's associate at NSF, "the universities would be forced to decide whether to modify their own policy, refuse to participate in the Foundation's program or secure their own funds for a supercomputer center. If there is no government money involved, there's not a whole lot that Washington can do to control who's to have access to university supercomputers—though the government can always deny or limit the visas of Soviet researchers who might want access to supercomputers."

SIGTT study. For its part, NSF has deferred pressing the centers to comply until a clear policy is in place. That may take some time. Through the summer a special task force of the Senior Interagency Group on Technology Transfer, which consists of the Secretaries of State, Defense, Commerce, Justice and Energy, along with the heads of NSF, NASA, the White House Office of Science and Technology Policy, Office of Management and Budget and the intelligence agencies, has been meeting nearly once a week to develop a consistent policy.

"There's an idea out there that thousands of scientists from countries that are potentially hostile now have unlimited access to supercomputers," says Kusinski. "The fact is that a relatively small number enter our country and an even smaller number have any use of supercomputers. The damage they could do is exaggerated—not that they couldn't do harm with unlimited access. But, it turns out, with time on supercomputers so scarce and costly, they get very little. Supercomputer time is jealously guarded. Yet there are probably foreign citizens with NSF contracts and grants who can purchase time on supercomputers from commercial providers like Boeing and United Computing. That's a loophole that will need to be sewn tight by any policy."

A member of the SIGTT working group, Donald J. Goldstein, director of the Pentagon's international economic trade and security policy, explains that the flurry over supercomputer access derives from Soviet bloc efforts to secure supercomputers, which are nonexistent in those countries. "We know that supercomputers are a target for the Soviets," he asserts. The policy eventually worked out by SIGTT will be designed to cover every supercomputer in the US. The intention of the White House and Pentagon is to extend the policy to friendly countries with supercomputers by way of bilateral agreements, which already exist with West Germany and Britain, to name two.

NSF's Herz says, "If I were guessing, I would say there's a highly plausible case for supercomputers to be covered by national security rules. . . . It's not so obvious that the answers here will be found in debates about traditional academic freedoms and national security concerns." —IG

in brief

The National Bureau of Standards and the Institut Laue–Langevin in Grenoble, France, have agreed to set up a five-year program of collaborative research to develop the use of cold neutron beams for materials research and related experimental work. The two institutions will organize exchanges with the objective of devising new instrumentation and techniques. □