pertise is in security. Is that appropriate for the Social Security Administration or for the Securities and Exchange Commission?" Adler also is concerned by the NSA's desire to encode all information that, although unclassified, is, to the agency's mind, sensitive. This includes economic and banking information, for example. "Just what kind of information doesn't have a national security element to it?" Adler asks.

Whitfield Diffie of BNR in Mountain View, California, is concerned by the proposed secrecy of the NSA's algorithms. He would feel more confident advising people to use them, he says, if he knew what they were. Diffie is among the first researchers outside the NSA to study cryptography and is an expert on communications security. Deeley says he has to keep the algorithms secret because "good algorithms are hard to come by." Why publish them, he says, and "give the other side a leg up?" Diffie responds, "I am not particularly persuaded that their algorithms are so fragile and I personally would much rather see publicly available algorithms used."

The NSA's new system would supersede the Data Encryption Standard, or DES, which is widely used both within and outside the government. The NSA feels it cannot continue to endorse the DES.

The DES was published about 10 years ago by the National Bureau of Standards for use by government agencies to protect nonclassified information. The code actually was developed by IBM researchers who consulted with the NSA. The DES is the only unclassified code approved by the NSA and it has taken over the encryption market. Barton O'Brien, who is vice president for sales of RSA Data Security, Inc., estimates that 98 or 99 percent of all the companies that sell encryption equipment in the United States sell the DES. And, says Deeley, "DES is sophisticated. DES is damn good." Although researchers outside the NSA have spent the past decade trying to break the DES, none have succeeded.

But the problem with the DES, according to Deeley, is that it is too popular. It is used by the military, by government agencies, by banks, by corporations. "When you have a standard that you've published and that has been around for a long time and that is now used by everybody and his brother, we get concerned that it has become a sufficiently lucrative target that another government might throw a lot of resources at it," says Deeley. Does that mean that the Soviet Union can break the DES? "I wouldn't bet a plugged nickel on the Soviet Union not breaking it," Deeley responds.

In 1988, the DES is scheduled to be re-approved by the NSA for use through 1993. But, says Deeley, "I won't do it." Instead, the agency will provide its new, secret, algorithms.

Deeley acknowledges that the new computer chips will be designed to prevent reverse engineering but is reluctant to say just how that would be done. "There are a variety of techniques and if you wanted to invest time and money, you could protect chips," he remarks. The chips could be coated with a material that could not be removed without destroying the chips themselves. Or the chips could self-destruct if they are tampered with. Or they could be designed as a puzzle so intricate that it is nearly impossible to reconstruct the encryption algorithms from examining the chips. But it certainly would not be to the NSA's advantage to give away its chip-protection secrets. "Let them play with the chips. Let them dissipate their energies trying to get us," says Deeley.

According to Deeley, the NSA will supply a variety of algorithms as part of its new program, but the exact number is secret. "We will use as few algorithms as possible," he notes. "We will try to provide a very few very good ones."

Despite the qualms of the NSA's critics, it looks like the new program is well under way. Fleming is starting to talk to industry groups about it and he expects to have the first devices next year. So far, he says, the idea has met with enthusiasm. "It's exciting, it really is," he remarks. "There is a lot of interest, a lot of companies are calling us. We're on our way."—GINA KOLATA

Another Biotech Board Proposal

In August, the heads of several government agencies accepted a proposal to create a new Biotechnology Science Board that would have broad authority over research and development in genetic engineering (*Science*, 23 August, p. 736). Under the terms of that proposal, the biotech board would have been what amounts to a clone of the National Institutes of Health's Recombinant DNA Advisory Committee (RAC), with the likely potential of usurping most of the RAC's responsibilities. It would have been chartered out of the office of the assistant secretary for health in the Department of Health and Human Services.

Opposition from researchers and others to any administrative move that would undermine the RAC has now resulted in a new, alternative proposal for a biotechnology coordinating committee that would be chartered out of the White House Office of Science and Technology Policy. Instead of having the assistant secretary for health as its head, it would be chaired alternately by the directors of NIH and the National Science Foundation, according to Bernadine Healy, outgoing deputy director of OSTP who presented the new proposal to a meeting of the RAC on 23 September.

The proposed board "will be constituted as an interagency coordinating council," Healy wrote in a letter to Senator Albert Gore (D-Tenn.) who had opposed the previous plan, in large part because it would have undercut the RAC's authority over human gene therapy, an issue to which it has already given a good deal of study. According to an aide to Gore, the Senator is not yet prepared to respond to this second proposal but will once he has had a chance to study it.

The biotech board as currently envisioned would be made up exclusively of government agency officials who would not become engaged in the kinds of detailed analyses of issues that are conducted by the RAC and other agency review committees. Nor would the board's meetings or minutes be open to the public, an aspect of the new proposal that has already raised opposition. However, general reaction to the proposal from people at the RAC meeting can be described as cautiously favorable. "It certainly is an improvement over the Biotechnology Science Board idea," said one observer. Details about the new plan will be released shortly for public comment.

—BARBARA J. CULLITON