LETTERS

NBS: Problems and Needs

Gina Bari Kolata's article "National Bureau of Standards: A fall from grace" (News and Comment, 2 Sept., p. 968) gives an inaccurate picture of NBS. While the perceptive reader would recognize the inherent inconsistency of the article's title with the fact that 15 new assignments have been given to NBS by Congress since 1965, the reader would have to be well informed to note that, except for minor references, the work of two of the four institutes of the Bureau is ignored. Specific examples can be cited of current research at NBS that is of top quality and has significant basic and applied aspects.

The Fire Prevention and Control Act of 1974 gave the Bureau a broad mandate for research in fire safety. The NBS program includes high-quality research on toxicological effects of combustion products, chemical kinetics, and gas dynamics which is making the United States a world leader in an area where previously the best research was done in Japan and the United Kingdom. No effort is being made to hide this research, and NBS has attracted staff members of outstanding quality to this program.

Under the Brooks Act of 1965, NBS was given the responsibility of resolving many issues associated with the rapidly increasing usage of computers. Important NBS accomplishments include the first data encryption standard, the first validation system for software, and pioneering work in robotics.

A third example of current research at NBS relates to the more efficient use of energy. For a number of years preceding the national recognition of the energy crisis, NBS had carried out a systematic investigation of the thermal characteristics of building materials and building systems. While the importance and significance of this work has recently been widely recognized and has resulted in the promulgation of a nationally accepted standard for energy conservation in buildings, it was openly supported for many years before the Organization of Petroleum Exporting Countries or the Energy Research and Development Administration were organized.

Kolata's article emphasizes one very valid point: NBS does have severe problems and urgent needs. It needs vigorous and perceptive management; it needs a position in the hierarchy of federal executive agencies where its potential for public service is more clearly recognized; and it needs an audience in the Office of Management and Budget that can accurately perceive its capabilities.

Congress has recognized the solid achievements of NBS by giving it a number of challenging assignments. Thus, it has put the Bureau in the position to make even greater contributions in the future. But it also needs a better public recognition of both its capabilities and problems. The last need can be partially met by *Science*. We urge *Science* to publish a balanced article on NBS. We have recently completed a total of more than 12 years as senior NBS managers and would be happy to assist.

F. KARL WILLENBROCK
School of Engineering and Applied Science, Southern Methodist University, Dallas, Texas 75275

RUTH M. DAVIS
Research and Advanced Technology, Department of Defense, The Pentagon, Washington, D.C. 20301

Some of the National Bureau of Standards' problems are unique, but many of those detailed in Kolata's article are familiar to persons acquainted with federal (civil service) laboratories.

For more than 6 years, federal laboratories have experienced (i) static or declining budgets; (ii) especially rough treatment of basic research (the term has been replaced by "technology base" in the Defense Department lexicon); (iii) layoffs, and, in a number of cases, closings; (iv) deterioration of morale; (v) drift of many of the best workers to other jobs, many of them leaving science altogether; (vi) enlargement of their responsibilities, even as their resources diminish; (vii) strident demands for immediate payoffs and "visibility"; and (viii) increased managerial "oversight" of details, with concomitant increases in the amount of paperwork and the number of required briefings.

The plight of federal laboratories has largely gone unreported, whereas the ups and downs of universities and federal granting agencies have been deemed newsworthy. Shortly after the Carter Administration took office a spate of articles and editorials in professional magazines appeared, urging changes in federal science policies. The authors wrote from an almost exclusively academic frame of reference, with the universities cast as virtually the sole performers of scientific research (especially basic research), and the federal government being simply the source of largesse and red tape.

I would like to make what unfortunately seems to be a revolutionary suggestion: those who urge better support of scientific research should do just that—support scientific research, and not only research in one or two kinds of institutions. Our interests as scientists transcend institutional boundaries, and so do our difficulties. It is no coincidence, for example, that the above list of federal lab woes is so similar to the lament heard from university, industrial, and federally funded independent laboratories.

Scientific research will return to good health only when fellow scientists are regarded as colleagues and allies, and not as unwanted competition for research support.

MICHAEL N. ALEXANDER
60 Williams Road, Lexington, Massachusetts 02173

Computer Encryption: Key Size

W. L. Tuchman's comments (Letters, 2 Sept., p. 938) on Gina Bari Kolata's article "Computer encryption and the National Security Agency [NSA] connection" (News and Comment, 29 July, p. 438) may be better understood when it is realized that IBM seems to distinguish between the choice of a key size for the DES (Data Encryption Standard) and the design of the algorithm itself. In this parlance, Tuchman does not contradict Kolata's article when he says that "In no way did NSA affect the design of the algorithm." And Tuchman implicitly confirms NSA's role when he says, "Our involvement with NSA was limited to obtaining permission to export computer equipment incorporating the DES." It is known that NSA would not allow an encryption standard with a larger key size to be exported. (Several times I was warned by supporters of the current standard to abandon my request for a larger key size because it would prevent export of the device.)

I am sympathetic to the dilemma in which IBM appears to find itself—caught between NSA and the public. But with its current position, IBM may be assuming full responsibility for the security of the DES algorithm, including its key size. Acceptance or refusal by IBM of this responsibility would help resolve the issue.

I am also aware of NSA's needs for communication intelligence through cryptanalysis and understand the problems that a more secure standard might cause. I do not agree, however, that NSA should decide whether its needs or those of the civilian sector should take precedence. The lack of checks and balances is dangerous.

MARTIN E. HELLMAN
Department of Electrical Engineering, Stanford University, Stanford, California 94305