



Office of the Vice President, Intellectual Property & Licensing Services

500 Columbus Avenue, Thornwood, New York 10594

April 28, 1998

Mr. Stuart W. Katzke
NIST North (820), Room 427
Gathersburg, MD 20899

Dear Mr. Katzke:

IBM is pleased to respond affirmatively to NIST's "Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)." As you know, IBM is concerned that some of the language used in the license agreement pertaining to the AES candidate algorithm submission may be susceptible to more than one interpretation. Thus, the purpose of this letter is to state IBM's understanding of the NIST position and seek NIST's agreement that our understanding of the license language is correct. To that end, I have outlined the areas of concern along with our understanding of what is meant by the language.

1. Section 2.D.1, paragraph 3, sentence 4, contains the words "...I have fully disclosed all patents and patent applications *relating to* my algorithm." We are concerned that there could be many patents which could broadly be considered as "*relating to*" an algorithm which is eventually implemented in software or hardware in a computer. We presume that NIST did not intend that patents in such areas as microelectronics, board circuitry, or operating systems - to name a few - would be included in the patent grant. Therefore, the only patents which are deemed to "relate to" the algorithm are those which have claims which are necessarily infringed by the implementation of the algorithm which was adopted as the AES.

2. With regard to the words "...agree to grant the same rights in any other patent granted...." in Section 2.D.2, last sentence, particularly with respect to possible future patents issued on an improvement, we presume that NIST intended that a grant to such patents would only be required if the improvement is formally submitted to NIST (with a new license grant) during the review period and the improvement is incorporated into or becomes the formal standard. Thus, should an improvement be identified by IBM, formally be submitted to NIST and be incorporated into or become the AES, any patent rights to that improvement would be consistent with IBM's understandings expressed in item 1. That is, the grant would be to patents having claims which are necessarily infringed by the implementation of the improved algorithm in or as the AES.

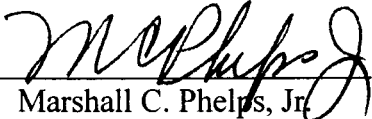
We would appreciate NIST's agreement that our interpretations of the two points above is correct and in accordance with NIST's understandings and intent. If so, please so indicate by having one of the duplicate copies of this letter signed on behalf of NIST and returned to me.

We understand that you might wish to make other potential submitters aware of these interpretations and thus give NIST permission to make this letter available to the public.

Thank you.

Very truly yours,

INTERNATIONAL BUSINESS
MACHINES CORPORATION

By 
Marshall C. Phelps, Jr.

Concurred

NIST

By 