FEDERAL RESERVE INFORMATION TECHNOLOGY

BRUCE J. SUMMERS
DIRECTOR

May 31, 2000

Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, STOP 8930
Gaithersburg, MD, 20899-8930

Attn: AES Finalist Comments (Bldg.820, Room 423)

Gentlemen:

The Federal Reserve Banks have been longstanding users and proponents of strong cryptography within the financial services community. As such, we would like to offer the following comments on the adoption of a replacement for the current Data Encryption Standard. The Federal Reserve believes that the selection of a replacement algorithm under the Advanced Encryption Standard (AES) program is of paramount importance to both the worldwide community of users of cryptographic technology and the United States financial community in particular.

It is our opinion that the selection of two algorithms (one primary and one backup) within the AES program would provide for an additional level of security should the need arise to replace the primary algorithm due to compromise. As do many organizations, we currently support multiple algorithms; thus, a two-algorithm scheme would not necessarily encumber our operating environment. We feel strongly, however, that for purposes of cost efficiency both algorithms should be built into products and platforms using this technology wherever possible. Should NIST make a decision to select two algorithms, it would be our preference that the selections utilize different cryptographic techniques to minimize the potential for possible compromise of the optional algorithm.

The initial call by NIST for submission of candidate algorithms for the AES listed several requirements, including 1) security; 2) cost; 3) algorithm and implementation characteristics; 4) hardware and software suitability; and, 5) simplicity. All of the finalist algorithms have met the first requirement; therefore, the selection of the winning algorithm(s) will be based on the remaining requirements. The Federal Reserve believes that, from an operational perspective, these requirements should be prioritized as follows: algorithm and implementation characteristics; cost; hardware and software suitability; and, simplicity. The selection of the winning algorithm(s) should be based on each algorithm's ability to satisfy these requirements in the order listed.

Thank you for the opportunity to comment on this very important issue.

Sincerely yours,