From: James.Downes@cio.treas.gov
Subject: AES Comments Round Two
To: AESround2@nist.gov
Cc: fbi09@earthlink.net, callahan@nlecc.gov, bacaldwell@atfhq.atf.treas.gov,
jaustin@tiscom.uscg.mil, Rick.Murphy@cio.treas.gov,
dmsiegle@earthlink.net, twhayton@aol.com
Date: Mon, 15 May 2000 21:17:52 GMT
X-MIMETrack: Serialize by Router on CIOMAIL/CIO/TREAS/GOV(Release 5.0a |May 4, 1999) at
05/15/2000 05:18:09 PM

The attached memo is provided for your consideration during selection of the Advanced Encryption Standard (AES) algorithm(s) on behalf of the Federal Law Enforcement Wireless Users Group (FLEWUG).

Any questions should be directed to me at (202) 622-1582 or via e-mail. We thank you for the opportunity to provide comments regarding this very important activity.

(See attached file: NIST Memo AES 2nd Round Comments 15May00.doc)

Jim Downes
Chair, FLEWUG INFOSEC Task Group

From: James.Downes@cio.treas.gov
Subject: Revised Memo from FLEWUG
To: AESround2@nist.gov
Cc: fbi09@earthlink.net, callahan@nlecc.gov, jaustin@tiscom.uscg.mil,
bacaldwell@atfhq.atf.treas.gov, Dwight.Locke@cio.treas.gov
Date: Mon, 15 May 2000 21:44:11 GMT
X-MIMETrack: Serialize by Router on CIOMAIL/CIO/TREAS/GOV(Release 5.0a |May 4, 1999) at
05/15/2000 05:44:24 PM

The Memo submitted on behalf of the FLEWUG should be amended as follows:

The third item listed should read " Due to working in a wireless environment, the algorithm must support relatively fast synchronization (vice synchronous) times.

The attached memo reflects this change.

(See attached file: NIST Memo AES 2nd Round Comments 15May00 Rev2.doc)

Jim Downes

May 15, 2000

MEMORANDUM FOR NIST
Via e-mail to AESround2@nist.gov

FROM: Jim Downes
Chair, Federal Law Enforcement Wireless Users Group (FLEWUG)
INFOSEC Task Group

SUBJECT: Second Round Comments-Advanced Encryption Standard (AES)

On behalf of the Federal Law Enforcement Wireless Users group (FLEWUG), comments are provided concerning the development of the Federal Information Processing Standard (FIPS) for the Advanced Encryption Standard (AES) for your consideration.

The FLEWUG member agencies are users of wireless equipment and currently use the standardized encryption algorithms to satisfy their particular operational needs. As the FIPS for AES is selected and published, the member agencies will transition to this new encryption algorithm from the current DES algorithms. Therefore, the comments provided are more from the user perspective than a technical evaluation of the algorithms.

The following comments are offered for your review and consideration:

1. It is of the utmost importance to ensure the algorithm selected has the robustness to work in a wireless environment. Wireless environments must deal with RF (radio frequency) interference issues that typically are not an issue in “wire-line” systems.
2. The AES algorithm must maintain the ability to utilize Over-The-Air-Rekeying (OTAR). We feel strongly that OTAR is a requirement that must be addressed in the AES documentation This capability is essential to the successful completion of the public safety related missions of the FLEWUG members. Additionally, a standardized key-fill protocol should be developed.
3. Due to working in a wireless environment, the algorithm must support relatively fast synchronization times.
4. The use of battery powered portable (hand-held) units dictates low power consumption. Portable equipment size will impact the space required to implement the algorithm in DSP or hardware.
5. The scalability of key lengths dictates an even more pressing need to implement the algorithms in software with reprogramming capabilities. The flexibility of software implementation will allow long term, low cost use of the selected algorithm on future generation wireless platforms.

Please direct any questions in this matter to me at (202) 622-1582 or via e-mail at james.downes@cio.treas.gov. We thank you for the opportunity to provide our comments pertaining to this important matter.

Cc: FLEWUG INFOSEC Task Group Members
FLEWUG Co-chairs