NEC Corporation
1753 Shimonumabe, Nakahara-Ku, Kawasaki, Kanagawa, JAPAN
e-mail: k-minematsu@ah.jp.nec.com

January 14, 2012

Dear NIST,

I have sent a security evaluation report on EAXprime (or EAX'), a blockcipher mode specified in the ANSI C12.22 as the standard security function for the Smart Grid, to IACR ePrint. The report is now available at `http://eprint.iacr.org/2012/018`.

Our report shows a serious security flaw of EAXprime when inputs are quite short.

We have not checked if our attacks are applicable to the messaging protocols defined by ANSI C12.22. However, they clearly demonstrate the insecurity of EAXprime as a general-purpose authenticated encryption (AE). Hence I consider it is not adequate to include EAXprime in an NIST SP document, at least to define a general-purpose AE mode. I also recommend to clarify the practicability of our attacks against the ANSI C12.22 protocols.

Sincerely yours,

MINEMATSU Kazuhiko