SIIA Accelerating Innovation in
Technology, Data & Media

202.289.7442 1090 Vermont Ave NW Sixth Floor
www.siia.net Washington DC 20005-4905

Submitted via email: fipswithdrawal@nist.gov

March 2, 2015

Richard Cavanagh,
Acting Associate Director for Laboratory Programs
National Institute for Standards and Technology
100 Bureau Drive, MS 8930
Gaithersburg, MD 20899-8930

Dear Mr. Cavanagh,

On behalf of the Software & Information Industry Association (SIIA), I am writing in support of the proposal to withdraw Federal Information Processing Standards 185 (FIPS-185), also known as the Escrowed Encryption Standard (EES).

SIIA is the principal trade association for the software and digital information industries. The more than 700 software companies, data and analytics firms, information service companies, and digital publishers that make up our membership serve nearly every segment of society, including business, education, government, healthcare and consumers. As leaders in the global market for software and information products and services, they are drivers of innovation and economic strength—software alone contributes $425 billion to the U.S. economy and directly employs 2.5 million workers and supports millions of other jobs.

EES, a hardware-focused standard for encrypted communications that was intended to protect unclassified government and private sector communications, has been the subject of considerable concern among industry since it approved in 1994. Not only should this standard be withdrawn because it references the cryptographic algorithm “Skipjack” that is no longer approved for U.S. government use, but the proposed withdrawal is also a timely reminder that efforts by governments to require use of specific technologies that have not been developed in a transparent manner with broad input are misguided and not likely to succeed.

As pointed out by a leading cryptographer shortly after the standard was created "rogue applications defeat EES by making use of the cipher without the government 'back door.’"[1]

[1] Blaze, Matt; Protocol Failure in the Escrowed Encryption Standard; August 20, 1994.

Many others pointed out the distinct possibility that escrowed encryption keys could be likely obtained by unauthorized persons, and misused by overzealous government agencies.
In addition to the inherent flaws of EES, the lack of transparency and openness that permeated the process contributed significantly to its failure.

This proposal and immediate failure of EES influenced the cryptography debate for years. When NIST announced its challenge to replace the outdated Data Encryption Standard (DES) with a new Advanced Encryption Standard (AES), it designed a process that was open, transparent, and global. The process—and result—received notable praise from the cryptographic community, including from one of the losers and one of NIST's harshest critics in previous years, thereby increasing confidence.

Unfortunately, renewed discussions about encryption have repeated old misunderstandings. For instance, in recent weeks, a key leader in EU anti-terrorism efforts has, per media reports, called for consideration of "rules obliging Internet and telecommunications companies operating in the EU to provide ... access of the relevant national authorities to communications (i.e. share encryption keys)."

Withdrawal of FIPS-185, 20 years after its creation, is a useful reminder of it the many failures of the approach and might influence policymakers from going down that mistaken path again.

Sincerely yours,

Ken Wasch

Ken Wasch !
President !