



POSITION STATEMENT

ENCRYPTION POLICY

*Adopted by the IEEE-USA
Board of Directors, 20 June 2008*

IEEE-USA opposes legislation to restrict the creation, availability, or legitimate use of encryption, including strong encryption by U.S. firms, or by other U.S. organizations. IEEE-USA urges policy-makers to avoid placing restrictions on the creation, availability or use of cryptography in the United States, or by U.S. firms.

IEEE-USA strongly supports the important goals of public safety and protection against foreign and domestic threats. At the same time, we join with the National Research Council (NRC) in its support of broad availability of cryptography to all legitimate elements of U.S. society(1).

The availability of cryptography is essential for governmental, financial, medical and industrial operations, both domestic and international. Continued economic growth and leadership of key U.S. industries depends on it. Further, encryption can be a defense -- and strong encryption is often the best defense against what has come to be recognized as potential domestic and foreign "cyber terrorism." These facts directly argue for more widespread availability and use of cryptography, not less, and for incorporating it into U.S. products that compete in the global marketplace.

The United States has a leadership position in most aspects of encryption-creation and use, but the United States does not have a monopoly on either the technology or the ability to enhance it. It is unlikely that any restrictive legislation or regulations on U.S. firms and other organizations can achieve the stated goals of such restrictions. Strong encryption technology has legitimate commercial uses. The demand for encryption products will be satisfied, if not by U.S. companies, then by non-U.S. companies. If U.S. laws force future development of strong encryption technologies to be undertaken by non-U.S. firms, the technical know how, innovation, as well as the jobs that go hand-in-hand with them, will also take place and reside only in non-U.S. organizations.

Restrictions on the export or use of cryptography, including limitations on encryption strength or legally-mandated key escrow, are likely to have similar negative economic effects without providing any additional benefit to public safety or security efforts.

On the contrary, we judge that legislation proposed to date can, and is likely to:

- Have a negative impact on the U.S. economy, its infrastructure and national security
- Make U.S. institutions more vulnerable, to attack by criminals, terrorists and other malefactors, both domestic and foreign
- Have a negative impact on the encryption capability of U.S. firms, causing their capabilities gradually to decline, and perhaps even to atrophy
- Have a negative impact on U.S. firms currently active in world markets, as well as on products and services that depend on them for their efficacy.

This statement was developed by the IEEE-USA Committee on Communications Policy and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public-policy interests of the more than 215,000 engineers, scientists and allied professionals who are U.S. members of the IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of the IEEE or its other organizational units.

BACKGROUND

There is an ever-increasing amount of research and analysis that adds strength to the positive argument for continued development, availability and use of strong cryptography in the many legitimate and vital arenas of government; medicine; business, both for profit and not-for-profit; as well as industries of all kinds.

In particular, in the age of the Internet, commercial entities depend significantly on the availability of strong encryption. The efficient functioning of markets depends on market actors' confidence in their transactions. In particular, they need confidence that they are communicating with the appropriate authority (authentication); their communications are not tampered with; and, especially for electronic commerce, transactions cannot be repudiated. Strong encryption, properly applied, addresses all of these critical infrastructure activities. Banning the use of strong encryption, or mandating weak encryption, would impact our world position in commerce.

These objectives argue for more widespread availability and use of cryptography. The availability of cryptography is essential for internal industry operations, and for incorporation into products that must compete in the global marketplace. The arguments justifying restrictions on the creation, development and use of strong cryptography in the United States have been far from convincing. Legal limits have failed in their stated goal to prevent the global availability of cryptography. Currently, hundreds, even thousands, of encryption products are available worldwide. Many of these products are implemented in software, making them extremely portable. Algorithms previously prohibited by U.S. controls on cryptographic exports are readily available at multiple overseas locations to anyone with a computer and modem. U.S. limitations

on the use of encryption cannot stop the development and transfer of encryption-based security products. Encryption products with all levels of strength are widely available from multiple sources worldwide.

Restrictions on encryption technology are also not likely to provide any benefits to public safety. Encryption is likely to be used by criminals to protect their communications, but their use of encryption is not necessarily obvious. Encryption takes place through conventional and unconventional forms. The latter include steganography -- the hiding of messages within other messages -- which might be used to embed encrypted talk, coded communications and other techniques for covert communication not easily recognized as forms of strong encryption. Laws prohibiting the use of strong encryption, un-escrowed key encryption, or mandating the use of government supplied, secret algorithms would be of little use to law enforcement efforts against these latter approaches.

IEEE-USA strongly opposes legislation to restrict the creation and legitimate use of encryption, including strong encryption, by U.S. firms and other organizations.

NOTES

(1) See Kenneth W. Dam and Herbert S. Lin, Eds., "Cryptography's Role in Securing the Information Society," Committee to Study National Cryptography Policy, National Research Council (1996). <http://www.nap.edu/books/0309054753/html/index.html>