



POSITION STATEMENT

ENCRYPTION POLICY

*Adopted by the IEEE-USA
Board of Directors, 18 Nov. 2011*

IEEE-USA urges policymakers to avoid placing restrictions on the creation, availability, or use of cryptography in the United States, or by U.S. firms. Because the integrity of an encryption capability inherently does not allow for “back doors” or third-party interception, IEEE-USA urges legislators and regulators to avoid weakening U.S. national and economic security by requiring such capabilities on Internet applications.

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. society¹. In addition, we agree with the National Institute of Standards and Technology (NIST) in their assertion that encryption is a key component of information security². Moreover, we join with the National Security Agency (NSA) in its urging to ensure that information technology (IT) systems and communications systems do not present unexpected intercept points.³

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 depend 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 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.

IEEE-USA believes that most general encryption legislative solutions proposed to date can, and are likely to, have a negative impact on the U.S. economy, its infrastructure and national security by:

- Creating potential systemic cybersecurity vulnerabilities, via “back door,” key escrow, or other special accesses originally designed for enforcement/intelligence agencies--but which might be exploited as rapid changes in methods--that challenge the ability to protect legacy systems
- Making U.S. institutions more vulnerable to attack by criminals, terrorists, and other malefactors, both domestic and foreign, by limiting the availability of emerging strong encryption and security breakthroughs within the United States
- Impairing the competitive leadership of U.S. firms, by causing encryption capabilities decline, and perhaps even atrophy, as off-shore competitors step up to provide strong encryption products
- Creating “cyber-uncertainty” for 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 210,000 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

An ever-increasing amount of research and analysis 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; and smart grid; 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 entities' 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, mandating weak encryption, or mandating impaired 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 Internet access. 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. Strong 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 includes 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. For that matter, such technology as one-time pads, in use since 1917 and probably unbreakable in the 1940s, have become considerably simpler to implement using modern technology. Laws prohibiting the use of strong encryption, un-escrowed key encryption, mandating the use of government supplied, secret algorithms, or mandating impaired encryption methods that structurally include the provision for a man-in-the-middle attack, would be of little use to law enforcement efforts against these latter approaches.

To promote more effective use of encryption, it would be very helpful if government fostered open discussion of how encryption can better protect the data transmitted over and stored in our critical IT infrastructure. Today, most companies can't ascertain which encryption technologies would actually be able to protect their data and systems from corporate or state-sponsored cyber-espionage. A National Research Council report⁴ highlighted how useful discussions of encryption, cybersecurity and cyberwarfare do not require disclosure of classified information.

Mandating services with built-in decryption capability may appear to enhance national security by enabling law enforcement and intelligence agencies the ability to intercept illicit communications. IEEE-USA supports the important goal of enhancing the tool kits for our nation's law enforcement and intelligence agencies. However, mandating built-in decryption to communications actually serves criminals and terrorists. Criminals and terrorists are likely to use strong encryption, even when communicating over weakly encrypted channels, such as instant messaging, or voice calls. However, any system with a built-in "back door" invites criminals and foreign intelligence services to attack legitimate, protected communications. From a technology perspective, there is no difference between a "back door," and what is known as a "man-in-the-middle" attack. In the "man-in-the-middle" attack, the attacker poses as the legitimate recipient of the communication. In the presence of "back doors," the attacker poses as the legitimate intercept point.

Weakening a communication protocol to enable interception is technically indistinguishable from enabling that protocol to be intercepted by criminals, terrorists, or foreign intelligence services. Such interception can disrupt commerce through legitimate user concern over security; present homeland security issues, if public safety communications are intercepted; and result in companies falling out of compliance with consumer privacy and corporate governance laws and regulations, such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA) and associated regulations, and the Payment Card Industry (PCI) Data Security Standard (DSS).

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>

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>

² See "Recommended Security Controls for Federal Information Systems and Organizations," Joint Task Force Transformation Initiative: Information Security, 2009. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>

³ See “Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components,” National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme for IT Security (NIST and NSA) 2009. http://www.niap-ccevs.org/cc_docs/CCPART2V3.1R3.pdf

⁴ See William A. Owens, Kenneth W. Dam, and Herbert S. Lin, Eds., “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,” Committee on Offensive Information Warfare, National Research Council (2009). http://www.nap.edu/catalog.php?record_id=12651