Calendar No. 263

106TH CONGRESS *1st Session*	SENATE	REPORT 106–142

PROMOTE RELIABLE ON-LINE TRANSACTIONS TO ENCOURAGE COMMERCE AND TRADE (PROTECT) ACT OF 1999

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 798

together with

ADDITIONAL VIEWS

AUGUST 5, 1999.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

69–010 WASHINGTON : 1999

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina
CONRAD BURNS, Montana	DANIEL K. INOUYE, Hawaii
SLADE GORTON, Washington	JOHN D. ROCKEFELLER IV, West Virginia
TRENT LOTT, Mississippi	JOHN F. KERRY, Massachusetts
KAY BAILEY HUTCHISON, Texas	JOHN B. BREAUX, Louisiana
OLYMPIA SNOWE, Maine	RICHARD H. BRYAN, Nevada
JOHN ASHCROFT, Missouri	BYRON L. DORGAN, North Dakota
BILL FRIST, Tennessee	RON WYDEN, Oregon
SPENCER ABRAHAM, Michigan	MAX CLELAND, Georgia
SAM BROWNBACK, Kansas	

MARK BUSE, *Staff Director*
MARTHA P. ALLBRIGHT, *General Counsel*
IVAN A. SCHLAGER, *Democratic Chief Counsel and Staff Director*
KEVIN D. KAYES, *Democratic General Counsel*

Calendar No. 263

106TH CONGRESS, 1st Session | SENATE | REPORT 106–142

PROMOTE RELIABLE ON-LINE TRANSACTIONS TO ENCOURAGE COMMERCE AND TRADE (PROTECT) ACT OF 1999

AUGUST 5, 1999.—Ordered to be printed

Mr. MCCAIN, from the Committee on Commerce, Science, and Transportation, submitted the following

REPORT

together with

ADDITIONAL VIEWS

[To accompany S. 798]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 798) "A Bill to promote electronic commerce by encouraging and facilitating the use of encryption in interstate commerce consistent with the protection of national security, and for other purposes", having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

PURPOSE OF THE BILL

The purposes of the bill are the following:

(1) Promoting electronic growth and fostering electronic commerce.

(2) Creating consumer confidence in electronic commerce.

(3) Meeting the needs of businesses and individuals using electronic networks.

(4) Preventing crime.

(5) Improving national security.

BACKGROUND AND NEEDS

GROWTH AND SIGNIFICANCE OF INFORMATION TECHNOLOGY INDUSTRY AND ELECTRONIC COMMERCE

The information technology (IT) industry is the true engine of economic growth in the United States. Responsible for approximately one-third of real growth in the U.S. economy, IT companies employ more than seven million Americans. The software industry alone in 1998, employed 806,900 people in the United States and generated $12.3 billion in direct tax revenue from their wages. Assuming software industry employment continues to grow at its long-term (1990 to 1998) trend rate, the software industry will directly employ more than 1.3 million people in the United States by 2008. Sales of software products and services in the United States in 1998 rose 17.8 percent to reach $140.9 billion. These numbers alone establish the IT industry as the driving force in our economy, providing economic development, employment opportunities, investment opportunities, expansion of the tax base, and the foundation for long-term economic growth.

The most significant contribution of the IT industry to the U.S. economy is in the area of exports and job creation. The rate of growth in industry employment has nearly doubled from 7.1 percent per year between 1990 and 1994 to 13.9 percent per year between 1994 and 1998. U.S. produced software comprises 70 percent of the world market. In 1997, the U.S.-owned packaged software segment of the core software industry contributed a surplus of $13 billion measured in retail value to the U.S. trade balance—an increase of 17.9 percent per year since 1990.

"The incredible growth of the industry and its exporting success benefits America through the creation of jobs here in the United States. Many of these jobs are in highly skilled and highly paid areas such as research and development, manufacturing and production, sales, marketing, professional services, custom programming, technical support and administrative functions. In the U.S. software industry, workers enjoy more than twice the average level of wages across the entire economy—$57,319 versus $27,845 per person."[1]

Much of the growth in consumer and business demand for IT products and services is driven by the explosive growth of the Internet. The last few years have seen a dramatic expansion in Internet connections, with more than a 13-fold increase in the Internet host computer count between 1994 and 1998. The Internet connects more than 29 million host computers in more than 250 countries. Currently, the Internet is growing at a rate of approximately 40 percent to 50 percent annually. Some estimates of number of U.S. Internet users are as high as 62 million. More than half the computers connected to the Internet reside in the United States. UUNet, an Internet access provider, estimates that Internet traffic is doubling every 100 days. Much of this new Internet activity is the result of business to business communications, and the increased on-line consumer activity. Recent years have seen a dra-

[1] Testimony, D. James Bidzos, Vice Chairman, Security Dynamics Technologies, Inc., Parent company of RSA Data Security, Inc., Senate Committee on Commerce, Science, and Transportation, Hearing on Encryption, June 10. 1999.

matic increase in the number of new businesses opening "on-line," and the number of existing businesses shifting commercial activity to the Internet.

A recent study estimated that revenues from online retailers in the U.S. and Canada will reach $36.6 billion for 1999, a 145 percent increase over 1998. The study projected that computer hardware and software retailer revenues will hit $7.4 billion, travel retailers $7.3 billion, financial brokerages $5.8 billion, collectible $5.4 billion.[2]

ADVANCED ENCRYPTION PRODUCTS CRITICAL TO CONTINUED GROWTH OF INFORMATION TECHNOLOGY INDUSTRY AND ELECTRONIC COMMERCE

"Today's information age requires U.S. businesses to compete on a global basis, sharing sensitive information with appropriate parties, while protecting against competitors, vandals, suppliers, customers, and foreign governments."[3] As business to business communications activity increasingly migrates to the Internet, seeking its speed and efficiencies, and Internet-based retail activity increases, attracted by low costs and access to global consumer markets, the demand for advanced encryption technology will continue to grow. The future of E-commerce, indeed, its very survival, is dependent upon the ability to maintain the integrity of confidential and proprietary data.

Much of the debate surrounding encryption export centers on the importance of market access to encryption technology producers. Market access is critical to the survival and growth of any industry. However, the critical nature of the need for encryption goes well beyond producers of such products. In an information age, advanced encryption is critical to all businesses.

"The global economy, tied together with the Internet, is turning businesses into virtual enterprises, localized products and global products, and geographically limited networks into worldwide networks * * * American businesses must be able to sell and support their products worldwide. American businesses must be able to securely communicate and coordinate with their foreign subsidiaries and business partners worldwide. American businesses must be able to conduct safe electronic commerce worldwide."[4]

ADVANCED ENCRYPTION PRODUCTS ARE GENERALLY AND WIDELY AVAILABLE IN THE GLOBAL MARKETPLACE

The rationale for strict export controls on advanced encryption products is rooted in the goal of protecting U.S. national security and law enforcement interests. The logic is that, by restricting U.S. exports of such products, the risk that advanced encryption products may be secured by foreign entities posing threats to such interests would be reduced. However, this logic breaks down in the face of the general and wide availability of advanced encryption products through foreign manufacturers and producers.

---

[2] "The State of Online Retailing 2.0," Boston Consulting Group for Shop.org, 1999.

[3] "Cryptography's Role in Securing the Information Society," Kenneth W. Dam and Herbert S. Lin, 1996.

[4] Testimony, David Aucsmith, Chief Security Architect, Intel Corporation, Senate Committee on Commerce, Science, and Transportation, Hearing on Encryption, June 10, 1999.

The worldwide ubiquity of encryption makes the technology impossible to control. Encryption techniques are taught to students in university and colleges in all countries. Informative papers on encryption are published annually at conferences held around the world. Knowledgeable encryption experts from outside the United States have developed encryption standards in widespread use today such as the IDEA algorithm from Switzerland which is the foundation for the encryption program PGP (Pretty Good Privacy) which is relied on by over 6 million people. In fact, these foreign experts are all competing with the U.S. encryption experts to establish the next generation U.S. encryption standard—the Advanced Encryption Standard.

A 1999 study, "Growing Development of Encryption Products in the Face of U.S. Export Regulation," identified 805 current hardware and/or software products incorporating cryptography manufactured in 35 countries other than the United States. These countries include the United Kingdom, Germany, Canada, Australia, Switzerland, Sweden, the Netherlands, and Israel. This represents 22 percent increase over the two-year period since 1997. At least 167 of the 805 products used strong encryption, defined as those which may not be exported from the United States under current regulations. The same study found that six additional countries had joined the group of encryption producers and exporters: Estonia, Iceland, Isle of Man, Romania, South Korea, and Turkey. Further, the report found a significant increase in the production volume of certain countries such as Germany, the U.K., Japan, and Mexico. There are now 512 foreign companies either manufacturing or distributing foreign-produced encryption products in 70 countries outside the United States.[5]

Clearly, foreign-based companies are emerging to meet the market demand for advanced encryption products. Equally clear, is that they are doing so at the expense of U.S. producers.[6] The study cited above "found examples of advertising used by non-U.S. companies that generally attempted to create the perception that purchasing American products may involve significant red tape and the encryption may not be strong enough due to export controls."[7]

The documented proliferation of options created by the general and wide availability of foreign manufactured and distributed encryption products underscored the futility of restricting export of similar U.S. manufactured products as a solution to legitimate national security and law enforcement objectives. In fact, such restrictions serve to undermine such objectives by threatening U.S. leadership in the area of encryption, thus aiding in the proliferation of non-U.S. options. The Committee believes that the greatest assurance of American national security and law enforcement objectives is to secure the absolute dominance of United States IT industries in the global marketplace.

---

[5] "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulation," Cyberspace Policy Institute, School of Engineering, The George Washington University, June 1999.

[6] Example: www.cyber.ee/infosecurity/products/privador/index.html, "American Products+red tape = weak encryption."

[7] Testimony, Professor Lance Hoffman Ph.D., The George Washington University, Senate Committee on Commerce, Science, and Transportation, Hearing on Encryption.

NATIONAL SECURITY AND LAW ENFORCEMENT CONCERNS ARE LEGITIMATE: KEY RECOVERY AND STRICT EXPORT CONTROLS ARE ILL-CONCEIVED

The benefits of encryption sought by legitimate private and business interests, may also be used to enhance the capabilities of those posing threats to U.S. national security and law enforcement interests. However, the solutions posed by the various agencies responsible for safe guarding these national interests ignore the realities of the marketplace and attempt to apply outdated approaches to a technology and business environment to which they are ill-fitted and ineffective. In fact, much of what is promoted as the solution, serves to undermine U.S. national interests in a digital age.

The primary approach advocated by the Justice Department is to promote recoverable encryption products. "Given both the benefits and risks posed by encryption, the Department (Department of Justice) believes that encouraging the use of recoverable products * * * is an important part of the Administration's balanced encryption policy."[8] By "encouraging," the Department means requiring the use of specified recoverable products in order for private citizens and businesses to interoperate with government computers. This represents, effectively, a backdoor federal mandate. The effect of such a mandate would be to dramatically skew the free market. Further, it would impose substantial costs on the private sector for those individuals and entities who would need to reconfigure existing systems, or establish dual systems.

The solutions posed by the various agencies responsible for safeguarding these national interests ignore the realities of the boundless nature of the Internet and the realities of the global marketplace. These policies attempt to apply outdated approaches to a technology and business environment that defies traditional approaches.

"If encryption can protect trade secret and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States."[9] Strong encryption products reduce crime. Thus, it should be the goal of U.S. policy to encourage the widespread use of such products.

"Information security is critical to the integrity, stability and health of individuals, corporations, and governments * * * Frankly, there is no substitute for good, widespread, strong cryptography when attempting to prevent crime and sabotage through these networks. The security of any network, however, is only as good as its weakest link. America's infrastructures cannot be protected if they

[8]Testimony, Department of Justice, Senate Committee on Commerce, Science and Transportation, Hearing on Encryption, June 10, 1999.

[9]"Cryptography's Role in Securing the Information Society," Kenneth W. Dam and Herber S. Lin, National Research Council, 1996.

are networked with foreign infrastructures using weak encryption." [10]

In support of this policy, the DoJ argues that there is already significant market demand for recoverable products. However, there is a substantial difference between the forces of consumer demand in the free market, and the invisible hand of a backdoor government mandate.

The National Security Agency (NSA) argues that U.S. policy must include strict controls over the export of strong encryption products. However, as previously stated, such controls will do little to prevent access to encryption by enemies of the state. In fact, such controls simply provide "room" in the encryption marketplace for foreign competitors. Many of these competitors exercise none of the restraint of U.S. manufacturers, and the U.S. government does not enjoy the benefit of the technical review provided under current regulation and included in the PROTECT Act.

ENCRYPTION EXPORT CONTROLS SHOULD BE INFORMATION-BASED AND RATIONAL

Industrial espionage poses a critical problem in a global marketplace. The National Counterintelligence Center has concluded that "specialized technical operations (including computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses) account for the largest portion of economic and industrial information lost by U.S. corporations." [11] As a result of this information security threat, it is absolutely critical that strong encryption technology be available to U.S. companies and their subsidiaries and partners around the world.

Decisions regarding export controls on advanced encryption products should be based upon the realities of the marketplace and reflect the global nature of information technology. Rationalizing and streamlining the process for approving the export of encryption products, while ensuring the best protection of law enforcement and national security interest is not a zero sum game. The PROTECT Act establishes a process when, viewed in the whole, ensures that decisions regarding the export of advanced encryption products are based on a comprehensive review of the foreign availability of similar products.

Under the Act, encryption products up to 64 bits are decontrolled. This is consistent with principles established under the Wassenaar Arrangement, an international encryption policy agreement signed by the United States and 33 other nations. The Act further provides for export or re-export of encryption products under license exception under certain conditions. These entities include publicly traded firms, government regulated firms, subsidiaries and affiliates of U.S. companies, firms audited under generally accepted accounting principles, strategic partners of U.S. companies, on-line merchants who use encryption to ensure the security of transactions, NATO, OECD and ASEAN member-nation

[10] Testimony, David Aucsmith, Chief Security Architect, Intel Corporation, Senate Committee on Commerce, Science, and Transportation, Hearing on Encryption, June 10, 1999.

[11] National Counterintelligence Center, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 1995.

governments, and for technology and services necessary to support such encryption technology.

ENCRYPTION EXPORT ADVISORY BOARD

The PROTECT Act establishes an Encryption Export Advisory Board. The purpose of this board is to review applications for export control exception for encryption products with key-lengths greater than 64 bits that do not qualify for exemption under the terms previously discussed. The Board is comprised of 12 members, eight individuals from the private sector with expertise in the IT industry, four from the government, specifically including representatives from the National Security Agency and the Central Intelligence Agency. The board would make recommendations to the Secretary of Commerce, who is granted full authority over encryption export control under the Act, for export exemption of encryption products where similar, foreign produced products are generally, and publicly available, or where such foreign produced products will be in the marketplace within 12 months.

One of the factors the Board will evaluate is whether an encryption product is a "mass-market" product. The term "mass-market" refers to products which are generally available, widely offered for sale, licensed or transferred to any person without restriction, which are intended for the user or purchaser to install without further substantial support by the manufacturer, but which are not designed, developed or tailored by the manufacturer for specific purchasers or users.

Mass market products are distributed through many channels, including OEMs, and are easily obtainable by consumers from numerous sources, including discount superstores, computer stores, and via the Internet. These products are easily transferable to individuals in foreign countries and cannot be controlled with any certainty. The PROTECT Act recognizes that generally available products are uncontrollable, and that once the product is deemed to be generally available, it should be easily exportable.

As previously stated, the national security rationale for restricting export of certain encryption products breaks down in the face of general availability of U.S. encryption products and foreign availability of encryption products comparable to U.S. products. The purpose of the Board is to put into place a reliable and consistent procedure for making such determinations. Upon the positive recommendation of the Board, the Secretary of Commerce would then have 30 days to approve or disapprove of the Board's recommendation. Should the Secretary fail to act within such timetables, the application for exception is deemed to be granted. Where the Secretary rejects the recommendation of the Board, such rejection is subject to judicial review.

Central to the Encryption Export Advisory Board approach, is that the Board must consider applications for export control exception on a product-by-product basis. This is critical. By framing the decision-making process in this way, assurance is provided the Board will be squarely on the cutting edge of marketplace development, and that the Board will not fall into a pattern of de facto standard setting.

Importantly, the PROTECT Act also provides a critical national security backstop. Regardless of the recommendations of the Board, or the decision of the Secretary, the President is granted the absolute authority to deny specific exports of encryption products to specific countries or individuals in order to protect U.S. national security interests. The President's decision is not subject to judicial review.

THE PROTECT ACT ENSURES THE PROTECTION OF NATIONAL SECURITY INTERESTS

The greatest guarantor of U.S. national security interests in a digital age is the complete dominance of the United States encryption producing industries. The PROTECT Act puts into place procedures to allow such industries to effectively compete for such dominance. However, the PROTECT Act reflects the legitimate concerns of both law enforcement and national security.

The Act clarifies that the U.S. government may continue to impose export controls on all encryption products to terrorist countries, and embargoed countries; that the U.S. government may continue to prohibit exports of particular encryption products to specific individuals, organizations, country, or countries; and that encryption products remain subject to all export controls imposed for any reason other than the existence of encryption in the product.

IMPROVING GOVERNMENT CAPABILITIES IN A DIGITAL AGE

A critical component of the PROTECT Act is improving the government's technological capabilities. Much of the concern from law enforcement and national security agencies is rooted in the unfortunate reality that the government lags desperately behind in its understanding of advanced technologies, and its ability to achieve goals and missions in the digital age. "The U.S. government should take steps to assist law enforcement and national security to adjust to new technical realities of the information age * * * High priority should be given research, development, and deployment of additional technical capabilities for law enforcement and national security use in coping with new technology challenges. Such R&D should be undertaken during the time that it will take for cryptography to become truly ubiquitous." [12]

This legislation expands NIST's Information Technology Laboratory duties to include: (a) obtaining information regarding the most current hardware, software, telecommunications and other capabilities to understand how to access information transmitted across networks; (b) researching and developing new and emerging techniques and technologies to facilitate access to communications and electronic information; (c) researching and developing methods to detect and prevent unwanted intrusions into commercial computer networks; (d) providing assistance in responding to information security threats at the request of other Federal agencies and law enforcement; (e) facilitating the development and adoption of "best in-

[12] "Cryptography's Role in Securing the Information Society," Kenneth W. Dam and Herbert S. Lin, National Research Council, 1996.Legislative History

formation security practices" between the agencies and the private sector.

The duties of the Computer System Security and Privacy Board are expanded to include providing a forum for communication and coordination between industry and the Federal government regarding information security issues, and fostering dissemination of general, nonproprietary and nonconfidential developments in important information security technologies to appropriate federal agencies.

LEGISLATIVE HISTORY

During the 106th Congress, on April 14, 1999, S. 798 was introduced by Senator McCain. Original co-sponsors of this bill, S.798, were Senators Burns, Wyden, Leahy, Abraham, and Kerry. Subsequently Senators Wellstone and Feingold were added as co-sponsors on June 22 and July 20 respectively. The bill was referred to the Senate Commerce Committee which held a hearing on the legislation on June 10, 1999. On June 23, 1999 the bill was reported favorably without amendment, by a voice vote, with Senator Stevens requesting to be recorded in the negative.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 9, 1999.

Hon. JOHN MCCAIN,
Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 798, the Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Hadley (for federal costs) and Shelley Finlayson (for the impact on state, local, and tribal governments).

Sincerely,

BARRY B. ANDERSON
(For Dan L. Crippen, Director).

S. 798—Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999

Summary: S. 798 would encourage the use of encryption technology in electronic commerce for domestic purposes and would allow exports of such technology with specified limits on the type of key used for encrypted products. (The term "key" refers to the mathematical code used to translate encrypted information back into its original, unencrypted format.) The effectiveness or strength

of contemporary encrypted algorithm. Under current policy, domestic producers may export encryption products with key lengths of up to 56 bits and stronger products for specified industries. S. 798 generally would allow domestic producers to export encryption products with key lengths of up to 64 bits and stronger products that are publicly available. The bill would require the National Institute of Standards and Technology (NIST) within the Department of Commerce (DOC) to select, by January 1, 2001, a standard for an encryption algorithm with a key length of at least 128 bits that would be available to anyone without charge. Upon adoption of the new standard, S. 798 would allow domestic producers to export products of strength comparable to that standard.

S. 798 also would require NIST to provide assistance and information on encryption products to law enforcement officials. In addition, the bill would prohibit states or the federal government from requiring individuals to relinquish the key to encryption products. Finally, the bill would establish an advisory board to determine which products should be publicly available.

Assuming the appropriation of the necessary amounts, CBO estimates that enacting this bill would result in additional discretionary spending by DOC of at least $25 million over the 2000–2004 period. Enacting S. 798 would not affect direct spending or receipts; therefore, pay-as-you-go procedures would not apply.

S. 798 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but would impose no costs on state, local, or tribal governments. The bill would preempt state laws that regulate specified aspects of the use of encryption products or services. The bill contains no new private-sector mandates as defined in UMRA.

Estimated cost of the Federal Government: CBO estimates that implementing S. 798 would increase discretionary costs for DOC by at least $5 million a year over the 2000–2004 period. The costs of this legislation fall within budget function 370 (commerce and housing credit).

S. 798 would require NIST to select an advanced encryption standard by January 1, 2001. Based on information from NIST, CBO estimates that completing the selection process would cost about $1 million a year in fiscal years 2000 and 2001, assuming appropriation of the necessary amounts.

S. 798 also would assign NIST a broad range of duties, including providing information and assistance, serving as an information clearinghouse, and conducting research. The costs to NIST would depend in part on the law enforcement community's need for help in decrypting certain communications and responding to security threats. Based on information from DOC, we estimate that the minimum costs to fulfill the bill's requirements would be $4 million to $5 million annually, but the costs could be much greater. Any spending by NIST would be subject to the availability of appropriations.

Under current policy, DOC's Bureau of Export Administration (BXA) would likely spend about $500,000 a year reviewing exports of encryption products. If S. 798 were enacted BXA would still be required to review requests to export encryption products. Thus, CBO estimates that implementing S. 798 would not significantly

change the costs to DOC to control exports of nonmilitary encryption products.

In coming years, advances in encryption and digital technology may substantially increase the costs of agencies responsible for law enforcement and national security. S. 798 would authorize appropriations of such sums as may be necessary to allow these agencies to complete their authorized tasks despite such advances. CBO estimates that the vast majority of these costs would be incurred under current law because law enforcement and national security agencies must already contend with highly effective forms of encryption developed by foreign producers. Any additional costs that would result from enacting S. 798 would be partially mitigated by the research required by the bill. CBO estimates that the net impact of the bill on agencies' costs for law enforcement and protection of national security are not likely to be significant.

Pay-as-you-go considerations: None.

Estimated impact on State, local, and tribal governments: S. 798 contains intergovernmental mandates as defined in UMRA, but CBO estimates that the costs would not be significant and would not exceed the threshold established by the act ($50 million in 1996, adjusted annually for inflation). The bill would preempt state laws that: (1) require encryption keys to be registered or accessible to the government; (2) authorize or require links between encryption products used for confidentiality and those used for authenticity or integrity; and (3) authorize the use of encryption products that do not interact with other commercially available encryption products. These preemptions would be mandates as defined in UMRA. However, states would bear no cost as a result of these mandates because none currently have such laws.

Estimated impact on the private sector: This bill would impose no new private-sector mandates as defined in UMRA.

Previous CBO estimates: On April 21, 1999, CBO transmitted a cost estimate for H.R. 850, the Security and Freedom Through Encryption (SAFE) Act, as ordered reported by the House Committee on the Judiciary on May 24, 1999. On July 1, 1999, CBO transmitted a cost estimate for H.R. 850 as ordered reported by the House Committee on Commerce on June 23, 1999. CBO estimated that the Judiciary Committee's version of H.R. 850 would cost between $3 million and $5 million over the 2000–2004 period and that the Commerce Committee's version of that bill would increase costs by at least $25 million the same period.

Estimate prepared by: Federal Costs: Mark Hadley. Impact on State, Local, and Tribal Governments: Shelly Finlayson.

Estimate approved by: Robert A. Sunshine, Deputy Assistant Director for Budget Analysis.

Regulatory Impact Statement

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

Because S. 798 does not create any new programs, but rather seeks to streamline the current regulatory process for approving the export of advanced encryption products, the legislation will have no additional regulatory impact, and will result in no addi-

tional reporting requirements. The legislation will have no further effect on the number or types of individuals and businesses regulated, the economic impact of such regulation, the personal privacy of affected individuals, or the paperwork required from such individuals and businesses.

The bill seeks to rationalize and provide certainty to the process of approval of the export of advanced encryption products. Such products are currently subject to burdensome, costly, and uncertain export control regulations. As such, the legislation does not create any new regulatory requirement.

SECTION-BY-SECTION ANALYSIS

TITLE I—DOMESTIC ENCRYPTION PROVISIONS

Section 101. Development and deployment of encryption—a voluntary private sector activity

This section provides that private sector use, development, manufacture, sale, distribution and import of encryption products, standards and services should be voluntary and market driven, and prevents the government from tying encryption used for confidentiality to encryption used for authentication.

Section 102. Sale and use of encryption lawful

This section makes it lawful for any person in the United States, and for any U.S. person in a foreign country, to develop, manufacture, sell, distribute, import, or use any encryption product.

Section 103. Mandatory government access to plaintext prohibited

This section prohibits government from setting standards or creating approvals or incentives for providing government access to plaintext. It also preserves existing authority for law enforcement and national security to obtain access to information under existing law.

TITLE II—GOVERNMENT PROCUREMENT

Section 201. Policy

This section states that it is the policy of the Federal government to permit the public to interact with the government through commercial networks and infrastructure and protect the privacy and security of any electronic communications and stored information obtained by the public.

Section 202. Federal purchases of encryption products

This section encourages government to purchase encryption products for its own use, ensures that such products will interoperate with other commercial encryption products, prohibits the government from requiring citizens to use a specific encryption product to interact with the government.

TITLE III—ADVANCED ENCRYPTION STANDARD

Section 301. Deadline for final selection of algorithm or algorithms by NIST

This section authorizes and directs NIST to complete establishment of the Advanced Encryption Standard by January 1, 2002, and ensures that the process is led by the private sector and open to comment.

Section 302. Commerce Department encryption standards and exports authority restricted

This section prohibits the Commerce Department from setting encryption standards (including through United States export controls) for private computers.

TITLE IV—IMPROVEMENT OF GOVERNMENTAL TECHNOLOGICAL CAPABILITY

Section 401. Information technology laboratory

This section expands NIST's Information Technology Laboratory duties to include the following:

(1) Obtaining information regarding the most current hardware, software, telecommunications and other capabilities to understand how to access information transmitted across networks.

(2) Researching and developing new and emerging techniques and technologies to facilitate access to communications and electronic information.

(3) Researching and developing methods to detect and prevent unwanted intrusions into commercial computer networks.

(4) Providing assistance in responding to information security threats at the request of other Federal agencies and law enforcement.

(5) Facilitating the development and adoption of "best information security practices" among the agencies and the private sector.

Section 402. Advisory board on computer system security and privacy

This section expands the duties of the Computer System Security and Privacy Board to include the following:

(1) Providing a forum for communication and coordination between industry and the Federal government regarding information security issues.

(2) Fostering dissemination of general, nonproprietary and nonconfidential developments in important information security technologies to appropriate Federal agencies.

Section 403. Authorization of appropriations

This section ensures that U.S. law enforcement agencies receive as much funds as are necessary to complete their missions and goals, regardless of technological advancements in encryption and digital technology.

TITLE V—EXPORT OF ENCRYPTION PRODUCTS

Section 501. Commercial encryption products covered

This section provides that the Secretary of Commerce has jurisdiction over commercial encryption products, except those specifically designed or modified for military use, including command and control and intelligence applications.

Section 502. Presidential authority

This section clarifies that the U.S. government may continue to impose export controls on all encryption products to terrorist countries, and embargoed countries and to prohibit exports of particular encryption products to specific individuals or organizations in a foreign country identified by the Secretary. It also clarifies that encryption products remain subject to all export controls imposed for any reason other than the existence of encryption in the product.

Section 503. Exportation of encryption products with not more than 64-bit key length

This section decontrols encryption products utilizing a key length of 64 bits or less.

Section 504. Exportability of certain encryption products under a license exception

This section permits exportability under license exceptions for the export or re-export of the following:

(1) Recoverable products.

(2) Encryption products to legitimate and responsible entities or organizations and their strategic partners, including on-line merchants.

(3) Encryption products sold or licensed to foreign governments that are members of NATO, ASEAN, and OECD.

(4) Computer hardware or computer software that does not itself provide encryption capabilities, but that incorporates APIs for interaction with encryption products.

(5) Technical assistance or technical data associated with the installation and maintenance of encryption products.

This section also provides that the Commerce Department must make encryption products and related computer services eligible for a license exception after a 15-day, one-time technical review. Exporters may export encryption products if no action is taken within the 15 day period.

Section 505. Exportability of encryption products employing a key length greater than 64 bits

This section permits encryption products to be exportable under license exception if the Secretary of Commerce determines that the product or service is exportable under the Export Administration Act or if the Encryption Export Advisory Board described in subsection (b) determines, and the Secretary agrees, that the product or service is generally available, publicly available, or a comparable encryption product is available, or will be available in 12 months, from a foreign supplier.

This section also creates an Encryption Export Advisory Board to make recommendations regarding general, public, and foreign availability to the Secretary of Commerce who must make such decisions. The Secretary's decision is subject to judicial review, and the President may override any decision of the Board or Secretary for purposes of national security without judicial review.

This section also ensures that the manufacturer or exporter of an encryption product may rely upon the Board's determination that the product is generally or publicly available or that a comparable foreign product is available and export the product without consequences.

This section also makes encryption products eligible for license exceptions after a one-time technical review, which must be processed within 15 days.

This section also grandfathers prior determinations by the Administration that encryption products with greater than a 64 bit key length are eligible for export.

Section 506. Exportability of encryption products employing AES or its equivalent

This section provides that, upon adoption of the AES, but not later than January 1, 2002, the Secretary must decontrol encryption products if the encryption employed is the AES or its equivalent.

Section 507. Elimination of exporting requirements

This section prohibits the Secretary from imposing any reporting requirements on any encryption product not subject to U.S. export controls or exported under a license exception.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman):

NATIONAL INSTITUTE OF STANDARDS OF STANDARDS AND TECHNOLOGY ACT

SEC. 20. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM. [15 U.S.C. 278g-3]

(a) The Institute shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(9) of title 44, United States Code;

(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and

privacy of sensitive information in Federal computer systems except—

(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(9) of title 44, United States Code; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

(b) In fulfilling subsection (a) of this section, the Institute is authorized—

(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

(2) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 5131 of the Clinger-Cohen Act of 1996 (40 USCS § 1441);

(3) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

(4) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; [and]

(5) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a)(3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign [policy.] *policy; and*

(6) to obtain information regarding the most current information security hardware, software, telecommunications, and other electronic capabilities;

(7) to research and develop new and emerging techniques and technologies to facilitate lawful access to communications and electronic information;

(8) to research and develop methods to detect and prevent unwanted intrusions into commercial computer networks, particularly those interconnected with computer systems of the United States government;

(9) to provide assistance in responding to information security threats and vulnerabilities at the request of other departments, agencies, and instrumentalities of the United States and State governments; and

(10) to facilitate the development and adoption of the best information security practices by departments, agencies, and instrumentalities of the United States, the States, and the private sector.

(c) For the purposes of—

(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

(2) performing research and conducting studies under subsection (b)(5), the Institute shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

(d) As used in this section—

(1) the term "computer system"—

(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

(B) includes—

(i) computers;

(ii) ancillary equipment;

(iii) software, firmware, and similar procedures;

(iv) services, including support services; and

(v) related resources;

(2) the term "Federal computer system" means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes informa-

tion (using a computer system) on behalf of the Federal Government to accomplish a Federal function;

(3) the term "operator of a Federal computer system" means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

(4) the term "sensitive information" means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

(5) the term "Federal agency" has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

SEC. 21. ESTABLISHMENT OF A COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORYBOARD. [15 U.S.C. 278g-4)

(a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

(b) The duties of the Board shall be—

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

(2) to provide a forum for communication and coordination between industry and the Federal Government regarding information security issues;

(3) to foster the aggregation and dissemination of general, nonproprietary, and non-confidential developments in important information security technologies, including encryption, by regularly reporting that information to appropriate Federal agencies to keep law enforcement and national security agencies abreast of emerging technologies so they are able effectively to meet their responsibilities;

[(2)] *(4)* to advise the Institute and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

[(3)] *(5)* to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

(c) The term of office of each member of the Board shall be four years, except that—

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the Institute or any other agency of the Federal Government with the consent of the head of the agency.

(g) As used in this section, the terms "computer system" and "Federal computer system" have the meanings given in section 20(d) of this Act.

ADDITIONAL VIEWS OF SENATOR HOLLINGS

This comprehensive rewrite of United States encryption control policy completes a multi-year effort by the Commerce Committee to update United States encryption export control policy. The legislation is an attempt to balance the legitimate interests of United States national security and law enforcement community while providing as much freedom as possible to U.S. providers of encryption software and hardware to sell their products overseas. The Committee's efforts have focused on achieving the most appropriate balance between these competing interests. While this legislation is not perfect, and both commercial and national security interests have expressed concern with the final product, the Committee is confident that the reported bill represents an appropriate balance under the current circumstances.

Aside from the commercial benefits for exporters of encryption products, the widespread dissemination of encryption technology will have a positive impact for additional development of electronic commerce and increased privacy and security of individuals and corporations. Increased computer security for legitimate users is an important and appropriate concern for this committee. Permitting stronger encryption products to be exported will increase the availability of more robust products in the United States, as it is more efficient to develop one global product. Nevertheless, we remain aware that illegitimate interests may seek to exploit encryption technology.

In order to ensure that the widespread distribution of encryption products does not have an injurious impact or will hamper our efforts to fight crime and terrorism will require a multifaceted effort. We must ensure that United States maintains our technological advantages in this area. This process will require increased efforts by Congress and the Administration. We must ensure that the Federal government provides the appropriate national security agencies with funding and statutory authority necessary to continue developing techniques and creative methods to decrypt intercepted items. We must also ensure smooth coordination between national experts and local authorities. Finally, commercial providers should assist these government authorities in their efforts. We intend to monitor developments in this area to ensure that the appropriate resources are provided and will continue to work with federal agencies to ensure that they are responsive to the needs of local law enforcement officials.

The international control of the powerful encryption technology will require a multinational effort with real and enforceable sanctions for violations of the international controls. This international effort recently received a boost from a multilateral agreement, the Wassenaar agreement, designed to place limits on the availability of such exports. To date, the effectiveness of this agreement to curb

the export of strong encryption products is in question. If the international community is unable to enforce the Wassenaar agreement and place meaningful international controls on encryption products, the Committee may have to revisit this issue.

ERNEST F. HOLLINGS.

○

Document No. 29