Program; to the Committee on Labor and Human Resources.

SUBMISSION OF CONCURRENT AND SENATE RESOLUTIONS

The following concurrent resolutions and Senate resolutions were read, and referred (or acted upon), as indicated:

By Mrs. FEINSTEIN (for herself, Mr. BROWNBACK, and Mr. GLENN):

S. Res. 227. A resolution to express the sense of the Senate regarding the May 11, 1998 Indian nuclear tests; to the Committee on Foreign Relations.

By Mr. WARNER (for himself and Mr. FORD):

S. Res. 228. A resolution to authorize the printing of a document entitled ''Washington's Farewell Address''; considered and agreed to.

By Ms. MOSELEY-BRAUN (for herself and Mr. DURBIN):

S. Res. 229. A resolution commemorating the 150th anniversary of the establishment of the Chicago Board of Trade; considered and agreed to.

By Mr. DODD (for himself and Mr. GRASSLEY):

S. Con. Res. 95. A concurrent resolution expressing the sense of Congress with respect to promoting coverage of individuals under long-term care insurance; to the Committee on Finance.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Ms. MIKULSKI (for herself, Mr. GLENN, and Mr. SARBANES):

S. 2064. A bill to prohibit the sale of naval vessels and Maritime Administration vessels for purposes of scrapping abroad, to establish a demonstration program relating to the breaking up of such vessels in United States shipyards, and for other purposes; to the Committee on Armed Services.

NAVAL VESSELS LEGISLATION

Ms. MIKULSKI. Mr. President, I wish to bring to the attention of the Senate that today I am introducing legislation to change the way we dispose of Navy ships that are no longer needed. I am proud to say that this bill is being cosponsored by my senior Senator, PAUL SARBANES, as well as the distinguished Senator from Ohio, Senator JOHN GLENN.

With the end of the cold war, the number of ships to be disposed of in the military arsenal is growing. There are 180 Navy and Maritime Administration ships waiting to be scrapped. These ships are difficult and dangerous to dismantle. They usually contain asbestos, PCBs, and lead paint. They were built long before we understood all of the environmental hazards associated with these materials.

I am prompted to offer this legislation because an issue was brought to my attention by a Pulitzer Prize-winning series of articles that appeared in the Baltimore Sun written by reporters Gary Cohn and Will Englund. They conducted a very thorough and rigorous investigation into the way we dispose of our Navy and maritime ships. They traveled around the country and around the world to see firsthand how our ships are dismantled.

I must advise the Senate that the way we do this is not being done in an honorable, environmentally sensitive, efficient way. I believe that when we have ships that have defended the United States of America, that were floating military bases, they should be retired with honor. When I unfold to you the horror stories that the Sun paper found, you will be shocked, and I hope you will join in the cosponsorship of my bill.

Let me recite from the Sun paper:

As the Navy sells off obsolete warships at the end of the cold war, a little known industry has grown up in America's depressed ports, and where the shipbreaking industry goes, pollution and injured workers are left in its wake.

Headline No. 1. No. 2:

The Pentagon repeatedly deals with shipbreakers with dismal records, then fails to keep watch as they leave health, environmental and legal problems in America's ports.

In terms of our own communities on the border in Brownsville, TX:

In this U.S. shipbreaking capital on the Mexican border, where labor and life are cheap, scrapping thrives amid official indifference.

And, I might say, danger.

Also, even more horrendous is the way we use the Third World to dump American ships: In India, the Sun paper found:

On a fetid beach, 35,000 men scrap the world's ships with little more than their bare hands. Despite wretched conditions—

And dangerous environmental situations.

I point out what this means close to home. Let me tell you some stories. In Baltimore:

Workers have been toiling in air thick with asbestos dust. In Baltimore, laborers scrapping the USS Coral Sea ripped asbestos insulation from the aircraft carrier with their bare hands. At times they had no respirators, standard equipment for asbestos work. [As we all know,] inhaling asbestos fibers can have . . . lethal consequences.

It was not limited to Baltimore. At Terminal Island, CA, 20 laborers were fired when they told Federal investigators how asbestos was being improperly stripped from Navy ships. In Baltimore, workers were ordered to stuff asbestos into a leaky barge to hide it from inspectors.

Dangerous substances from scrapped ships have polluted harbors, rivers and shorelines.

The Sun paper goes on to say:

A scrapyard along the Northeast Cape Fear River in Wilmington, NC, was contaminated by asbestos, oil and lead. ''That site looked like one of Dante's levels of hell,'' said David Heeter, a North Carolina assistant attorney general.

Ship scrappers frustrate regulators by constructing a maze of corporate names and moving frequently. The Defense Department has repeatedly sent ships to scrappers who have records of bankruptcies, fraud [and] payoffs. . . .

Because of downsizing, the Navy promised that this would be a bonanza, for amounts ranging from $15,000 to dismantle a destroyer—15 grand to dismantle a destroyer—to $1 million for an aircraft carrier.

They buy the rights to Navy ships, then sell the salvaged metal. . . .

Because of environmental violations and other issues, the Navy has had to take back 20 ships in yards in North Carolina, Rhode Island and California. . . . Of the 58 ships sold for scrapping since 1991, only 28 have been finished.

And, oh, my God, how they have been finished.

I would like to turn to my hometown of Baltimore. Mr. President, this is what the *Coral Sea* looked like while it was being dismantled in the Baltimore harbor. It looks like it was ravaged, like it was cannibalized. It looks like a tenement in a Third World area.

The Sun paper continues:

In Baltimore, torch handlers worked without other men on fire watch and without fire hoses. . . .

Picture yourself going out there trying to do that in the early morning.

The *Coral Sea*'s dismal end has been marked by stubborn fires and dumping of oil in the harbor, by lawsuits and repeated delays—but most of all, by the mishandling of asbestos.

Let me tell you that it was so bad that even a Navy inspector who came to look at what they were doing was scared to death to go on that ship because he was afraid it was too dangerous.

I am quoting the Sun paper.

On September 16, 1993, [the military] sent its lone inspector——

One inspector for the United States——

On his first visit to the Seawitch Salvage yard in Baltimore. . . . But Evans didn't inspect [it because]. . . . He thought it was too dangerous.

The next day, a 23-year-old worker named Alfio Leonardi Jr. found out how unsafe it would be.

He walked on a flight deck up in that situation and dropped 30 feet from the hangar.

I felt a burning feeling inside. . . . There was blood coming out of my month. I didn't think I was going to live.

He suffered a ruptured spleen, fractured pelvis, fractured vertebrae, and he broke his arms in several places.

The inspector was new to the job when the accident occurred. He had only 20 hours of training on environmental issues. He was not appropriately trained, and he didn't even know what shipbreaking was. At the same time, we had repeated fires breaking out.

In November of 1996, a fire broke out in the *Coral Sea* engine room. There was no one standing fire watch, no hose nearby. The blaze burned quickly out of control, and for the sixth time, Baltimore City's fire department had to come in and rescue the shipyard. At the same time, the owner of this shipyard had a record of environmental violations for which he ultimately went to jail.

We cannot tolerate this in the Baltimore harbor. If you look there, that is

where it is, right across from Ft. McHenry that defended the United States of America and won the second battle in the war of 1812. And look at it. That is what it looks like. It is a national disgrace that that was in the harbor as well as a national environment danger.

Right down the road was the Baltimore City Shipyard, the Bethlehem Steel Shipyard that was foraging for work. Another fighting lady from Maryland, Helen Bentley, our former Congresswoman—she and I and Senator PAUL SARBANES worked for Baltimore to be a home port. We were desperate for work in our shipyard—desperate. But no; do you think the Navy turned to shipyards like Bethlehem Steel? They turned to the rogues, the crooks, the scum, the scams, to dismantle our Navy ships.

I think the ships deserve more. I think the Baltimore harbor deserves more. And I think the United States of America deserves more. That is why I am introducing legislation to create a pilot project on how we can dispose of these ships, and in a way that is efficient, is orderly, and environmentally safe, and keeps the work in American shipyards, because while this was so terrible in my own home of Baltimore, MD, let me show you what was going on in the Third World.

This is the U.S. Navy ships being dismantled in India. Thirty-five thousand people work on a beach, often with no shoes, dismantling ships with their bare hands. This is so dangerous, in terms of what they are doing, that I believe it is an international disgrace. I was appalled we were also exporting our environmental problems overseas.

Mr. President, I called upon Secretary Cohen, when I read this series, to immediately stop what we were doing and to take a look. He did it. I want to thank him for his prompt response. He analyzed what they should do, and they made recommendations. But the recommendation was more enforcement of the same old way of doing business. Well, more enforcement of the same old way of doing business will still end up with the same old way of doing business—occupational safety dangers, environmental catastrophes, and a national disgrace.

So that is why I am introducing my own legislation. The first section of the legislation will absolutely ban the shipping, the sending of our 180 Navy ships overseas to be dismantled in such despicable situations. The other part establishes a pilot project for the U.S. Navy to look at how it could put our ships out for dismantling bids in American shipyards that meet environmental and occupational standards. Those shipyards, like the ones in my own hometown of Baltimore, that are fit for duty. They know how to build a ship. They know how to convert a ship. They know how to dismantle a ship.

I think the Navy can do better. The Navy has an outstanding record of dismantling nuclear submarines. They do it in a particular and unique way. They have the ingenuity and the technical competence, but they lack the will and the resources. What I hope my legislation will do is give them both the will and the resources to dismantle this in a way that retires our ships with honor. I knew that when the Senate saw those pictures they would be as taken aback as I have been.

I thank the Sun paper for their outstanding series in bringing this to not only my attention but to America's attention. They won the Pulitzer Prize. But I want the United States of America to be sure that we win an environmental victory here.

So, Mr. President, I am going to be introducing my legislation today as we speak. In fact, I send my legislation to the desk and ask that it be referred to the appropriate committees. I just want to close by saying that when we close military bases, we do it the right way, we pay to clean them up, we close them down and find other basic ways of recycling their use.

Every weekend I am around veterans who wear the ships on which they sailed. They have the U.S.S. Coral Sea; they have a variety of the ships that they sailed on. They are proud of those ships, and I am proud of those ships. And I am proud of the military. I conclude by saying, I thank Secretary Cohen for his leadership as well as Secretary Perry. They have done more environmentally positive things for the military than we have ever had done. But this is the next step.

I yield the floor, and I thank the Senate for its kind attention.

The PRESIDING OFFICER. The bill will be received and appropriately referred.

The Democratic leader.

Mr. DASCHLE. Mr. President, let me thank the distinguished Senator from Maryland for her eloquent statement. I appreciate her leadership. Her statement this morning is one that I wish the whole country could hear. Her leadership and her willingness to be involved in this issue is critical to all of us. And I appreciate so much her eloquence and the studious way in which she has pursued this matter.

By Mr. MURKOWSKI (for himself and Mr. STEVENS):

S. 2065. A bill to amend the Internal Revenue Code of 1986 to clarify the tax treatment of Settlement Trusts established pursuant to the Alaska Native Claims Settlement Act; to the Committee on Finance.

ALASKA NATIVE SETTLEMENT TRUST TAX LEGISLATION

Mr. MURKOWSKI. Mr. President, I am pleased to be joined by Senator STEVENS in introducing legislation that will allow Alaska Native Corporations to establish settlement trusts designed to promote the health, education, welfare and cultural heritage of Alaska Natives.

Mr. President, in 1987, the Alaska Native Claims Settlement Act was amended to permit Native Corporations to establish settlement trusts to hold lands and investments for the benefit of current and future generations of Alaska Natives. Assets in these trusts are insulated from business exposure and risks and can be invested to provide distributions of income to Native shareholders and their future generations.

Although the 1987 amendments were designed to facilitate the development of settlement trusts, many Native Corporations have been stymied in their efforts because the tax law, in many cases, imposes onerous penalties on the Native shareholders when the trusts are created. For example, when assets are transferred to the trust, they are treated as a *de facto* distribution of assets directly to the shareholders themselves to the extent of the corporation's earnings and profits.

Even though the current shareholders receive no actual income at the time of the transfer into the trust, they are liable for income taxes as if they received an actual distribution. This not only requires the shareholder to come up with money to pay taxes on a distribution he or she never received, but also can result in a situation where a trust fund beneficiary is required to prepay taxes on his share of the entire trust corpus, which may be substantially more in taxes than the amount of cash benefits he or she will actually receive in the future.

Our legislation remedies this inequity by requiring that a beneficiary of a settlement trust will be subject to taxation with respect to assets conveyed to the trust only when the actual distribution is received by the beneficiary. Moreover, the legislation provides that distributions from the trust will be taxable as ordinary income even if the distribution represents a return of capital. In addition, to ensure that these trusts do not accumulate excessive levels of the corporation's earnings, the legislation requires that the trust must annually distribute at least 55 percent of their taxable income.

Mr. President, Alaska Native Corporations are unique entities. Unlike Native American tribes in the lower 48, Alaska Native corporations are subject to income tax. But unlike ordinary C corporations, Alaska Native corporations have diverse purposes, one of which is to preserve and protect the heritage of the Native shareholders. The settlement trust concept is well suited to the special needs of Alaska's Natives. As the Conference Committee Report to ANSCA amendments of 1987 stated:

> Trust distributions may be used to fight poverty, provide food, shelter and clothing and served comparable economic welfare purposes. Additionally, cash distributions of trust income may be made on an across-the-board basis to the beneficiary population as part of the economic welfare function.

Settlement trusts will ensure that for generations to come, Native Alaskans will have a steady stream of income on which to continue building an economic base. The current tax rules discourage the creation of such trusts with the result that Native corporations are under extreme pressure to distribute all current earnings rather than prudently reinvesting for the future.

Mr. President, it is my hope that we will be able to see this legislation adopted into law this year. For the long-term benefit of Alaska Natives, this tax law change is fundamentally necessary.

By Mr. CHAFEE:

S. 2066. A bill to reduce exposure to environmental tobacco smoke; to the Committee on Environment and Public Works.

ENVIRONMENTAL TOBACCO SMOKE LEGISLATION

Mr. CHAFEE. Mr. President, today I am introducing legislation regarding one small aspect of the national tobacco debate. This bill addresses the problem of second-hand smoke, also known as Environmental Tobacco Smoke, or ETS for short. It is my hope that the ideas contained in this bill can be incorporated into any tobacco legislation acted on by the Senate.

The Committee on Environment and Public Works recently held a hearing on ETS at which we learned that the principal victims of second-hand smoke are children who live with smokers. Tobacco smoke has devastating consequences for children under 18 months of age. Annually, up to 15,000 infants are hospitalized for lung infections caused by ETS such as bronchitis and pneumonia. These severe lung infections claim the lives of hundreds of children each year.

Second-hand smoke is also responsible for less severe lung infections in 300,000 infants, 26,000 new cases of asthma among children, millions of middle ear infections, and roughly half the cases of Sudden Infant Death Syndrome (SIDS). These preventable illnesses, but 40 percent of children in one multi-State study were found to be routinely exposed to tobacco smoke.

The bill I am introducing today would assign some of the funds collected under any national tobacco settlement approved by Congress to a state grant program to educate parents about the dangers of smoking in the home. The statistics I just recited are not widely known by parents. Once aware of the profound risk ETS poses for their child, most parents will go to great lengths to protect their child, and I believe that even includes parents who smoke.

With the grant funds from this bill, States could provide information about ETS to pediatricians and other child care professionals for distribution to parents. States also could develop advertising aimed at parents. We only need to arm parents with information. They will do the rest.

This bill has a few other provisions. It affirmatively states that there is no federal preemption of State or local efforts to address ETS. It would ban smoking on international flights that originate or terminate in the United States. It also would extend and codify the President's Executive Order banning smoking in federal buildings. My good friend, Senator WARNER, in his capacity as Chairman of the Senate Rules Committee, is working to ban smoking from the public areas of the Senate. I applaud this effort and encourage my colleagues to support it. My legislation would complement his efforts in other federal buildings.

This bill does not address the question of smoking in private workplaces. Up to 3,000 adults die each year from lung cancer caused by ETS. Because of this statistic, some have argued that the federal government should ban smoking in nearly every building in the nation. Most legislative proposals on this issue would subject every dress shop and church hall in the nation to federal smoking regulations.

Ironically, most of those bills exempt bars and restaurants and other places where smoking can be common. That means they ignore the few places where employees faced a substantial threat from ETS while regulating every other workplace. I believe that there is a more efficient way to address workplaces with dangerous levels of ETS.

We should allow State and local governments to take the lead on this matter, but we also should help them to solve the problem. Some towns and States have taken action already. We can encourage more of them to do so by expanding the grant program described in my bill to reward States that reduce dangerous levels of ETS in the workplace. Incentive grants would allow States to tailor their solutions to address local concerns. Some States could seek a gradual ban while others may establish protective ventilation standards.

Any rule that requires changing a habit as deeply ingrained as smoking will be met with resistance. In contrast to a federal one-size-fits-all approach, State and local efforts can be tailored more easily to local concerns, and will, therefore, be more effective.

I did not address smoking in the workplace in my bill because I hope to work with other interested members to develop language that will be supportable on both sides of the aisle. Such a provision must both avoid rigid federal mandates and provide real incentives for States to address those workplaces with dangerous levels of ETS. I will continue to work with interested parties in an effort to devise such a provision. In the meantime, I wanted to offer the balance of my proposal for the Senate's consideration.

By Mr. ASHCROFT (for himself, Mr. LEAHY, Mr. BURNS, Mr. CRAIG, Mrs. BOXER, Mr. FAIRCLOTH, Mr. WYDEN, Mr. KEMPTHORNE, Mrs. MURRAY, and Mrs. HUTCHISON):

S. 2067. A bill to protect the privacy and constitutional rights of Americans, to establish standards and procedures regarding law enforcement access to decryption assistance for encrypted communications and stored electronic information, to affirm the rights of Americans to use and sell encryption products, and for other purposes; to the Committee on the Judiciary.

THE E-PRIVACY ACT

Mr. ASHCROFT. Mr. President, I rise to speak today on an issue that I find very important to the future of this country's leading position in the technology, and that is encryption. This issue has been under consideration since I first came to Capitol Hill, and for more than three years nothing has been accomplished by way of assistance to law enforcement, or to industry, or most importantly to the users of encryption in this country.

My first involvement in this entire discussion came about as a result of the need for protection and privacy. If we are to operate at our highest and best in the information age, instead of settling for something very far below our potential, we are going to need privacy and protection, and we are going to need the ability to operate with integrity on the Internet. The Internet has to be something more than speaking on the public square, it has to have the ability to allow individuals to communicate with each other. It has to have the same kind of rights and protections that are accorded to other aspects of communication. Without this privacy, the potential of the Internet is destroyed. In my judgment, the Internet would be destined to become just a sort of international bull session, nothing more than an international party line of commentary, or an international broadcast device. I do not believe it will fulfill its potential as a communication, entertainment, commercial and educational opportunity unless Internet communications are secure and the right of privacy is respected.

The Internet allows for the most participatory form of communications ever. In order for us to be able to both invite participation by everyone, and to be able to take advantage of it, we have to be able to exclude some parties from a particular communication. I do not know of any more successful exclusion technique in the electronic world than encryption, especially when so much information is going to be transmitted digitally, much of it through space as well as over hard lines of communication.

We have a tremendous potential for commerce on the Internet: everything from selling clothes, to real estate, to software itself. Electronic commerce has not reached its full potential, but it can. I think we've got a big agenda there, not just encryption but we've got to have legally binding signature legislation and therefore solid encryption.

Resisting efforts for mandatory domestic key recovery is also crucial. We have to remind ourselves that the Internet is like so much of the rest of the culture—government can't solve all the problems. At least we have to plead for restraint by those who would harm this technology. As I have said before, now is the time to draw a bright line against federal regulation of the computer industry. Washington must not start down the road of dreaming up regulations to fix problems that may or may not exist. Two things can be predicted with confidence about congressional meddling in this sector of the economy. First, legislation will be obsolete on the day it is passed. Second, it will hurt consumers, workers, shareholders, and the economy. If Congress had helped set up the transportation industry, there still might be a livery stable in every town, and buggy whip factories in large cities.

The irrationality of limiting the United States to levels of encryption which are far below what the world market is demanding and supplying in other settings, has been mind boggling. This legislation declares that American companies will be full and active participants in the encryption industry. Today, numerous editions of leading American designed and manufactured software bears the stamp, ''Not for sale outside the United States,'' because the software features robust encryption. That stamp does nothing to make Americans more secure, but it does provide aid and comfort to foreign competitors of American business. This legislation would eliminate that stamp once and for all.

Encryption, of course, is the most important issue to the future of electronic commerce and if we are to foster the integrity of the Internet we must have the means of communication domestically and international. I have to reaffirm that we must allow the software industry to compete in an international market where robust encryption already takes place. Months ago I went to a Commerce Committee meeting and took with me an ad from the Internet, which was from Seimens company in Germany advertising robust 128 bit encryption, saying that you can't get this from a U.S. manufacturer. The advertisement also indicated, however, that if you buy this you can use it in the United States and you can use it overseas as well, and, so if you want to have robust encryption buy it from Seimens. The Administration has decided to tie the hands of the U.S. encryption industry. To me that's a disaster, but it is also compounded by people beginning to develop relationships with foreign software providers as a result of the unavailability of 128 bit or robust encryption on the part of U.S. providers.

To see the Germans eagerly promoting this potential, and to have people from my own jurisdiction, from the state of Missouri, say, ''John, we have an office in Singapore, we have to be able to speak with them confidentially and communicate with them, and the government is making it impossible for us to send the encryption that we can use domestically. We can't send it to our office in Singapore because we are ineligible to export it.'' I don't want the situation to be such that I have to say, ''Well, go to Seimens in Germany.'' From Seimens you can buy the encryption that can be sent into the United States and from Seimens in Germany it can be sent to Singapore and so you can have your cake and eat it too by dealing with a non-domestic firm. For us to have a policy which provides for the slitting of our own throats, in a technology arena, where we have held the lead and must continue to hold the lead, I think is foolhardy to say the least. If we are to mark the next century as an ''American Century,'' or even to celebrate this week as high technology week in the Senate, we must be forward thinking and acting. This bill moves us away from antiquated export laws to a future in which American companies will be able to compete in the international marketplace without having one hand tied behind their back by the federal government.

This bill also clarifies the proper approach for encryption domestically as we move ahead in the digital age. The Administration and the FBI first indicated support for language that would mandate key recovery for all domestic encryption and now support several suggested approaches that would make using domestic key escrow a practical—though not legal—necessity. Director Freeh has gone so far as to mention the need for a new Fourth Amendment that considers the realities of the digital age. I think we need a new and improved approach to domestic encryption, not a new updated version of the Fourth Amendment. I, for one, am not eagerly awaiting the FBI's new release of Fourth Amendment 2.0 or First Amendment '98.

I think we have to work together to find a reasonable alternative to the current Administration policy and I think we have to ensure secure transactions. That's a clear responsibility. We can't have a situation where we don't have security and integrity in our business transactions. We have to be able to compete effectively in a worldwide marketplace. For us to limit our own potential in terms of competition makes no sense. We have to make sure that we don't allow those who would use information improperly or illegally to have access to it. That has to do with securing the transactions, and the integrity of the Internet as well.

This legislation is the solution to the problem. It is well thought out and attempts to address the legitimate concerns of all affected parties. I will seek passage of this legislation in this Congress and will commit the resources of my office that may be needed to achieve this end.

Business Week has recently reported that 61 percent of adults responded that they would be more likely to go on-line if the privacy of their information and communications would be protected. Mr. President, simply put, strong encryption means a strong economy. Mandatory access, by contrast, means weaker encryption and a less secure, and therefore less valuable, network.

I ask for unanimous consent that the entire bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 2067

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E–PRIVACY) Act''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Purposes.
Sec. 3. Findings.
Sec. 4. Definitions.

TITLE I—PRIVACY PROTECTION FOR COMMUNICATIONS AND ELECTRONIC INFORMATION

Sec. 101. Freedom to use encryption.
Sec. 102. Purchase and use of encryption products by the Federal Government.
Sec. 103. Enhanced privacy protection for information on computer networks.
Sec. 104. Government access to location information.
Sec. 105. Enhanced privacy protection for transactional information obtained from pen registers or trap and trace devices.

TITLE II—LAW ENFORCEMENT ASSISTANCE

Sec. 201. Encrypted wire or electronic communications and stored electronic communications.

TITLE III—EXPORTS OF ENCRYPTION PRODUCTS

Sec. 301. Commercial encryption products.
Sec. 302. License exception for mass market products.
Sec. 303. License exception for products without encryption capable of working with encryption products.
Sec. 304. License exception for product support and consulting services.
Sec. 305. License exception when comparable foreign products available.
Sec. 306. No export controls on encryption products used for nonconfidentiality purposes.
Sec. 307. Applicability of general export controls.
Sec. 308. Foreign trade barriers to United States products.

SEC. 2. PURPOSES.

The purposes of this Act are—

(1) to ensure that Americans have the maximum possible choice in encryption methods to protect the security, confidentiality, and privacy of their lawful wire and electronic communications and stored electronic information;

(2) to promote the privacy and constitutional rights of individuals and organizations in networked computer systems and other

digital environments, protect the confidentiality of information and security of critical infrastructure systems relied on by individuals, businesses and government agencies, and properly balance the needs of law enforcement to have the same access to electronic communications and information as under current law; and

(3) to establish privacy standards and procedures by which investigative or law enforcement officers may obtain decryption assistance for encrypted communications and stored electronic information.

SEC. 3. FINDINGS.

Congress finds that—

(1) the digitization of information and the explosion in the growth of computing and electronic networking offers tremendous potential benefits to the way Americans live, work, and are entertained, but also raises new threats to the privacy of American citizens and the competitiveness of American businesses;

(2) a secure, private, and trusted national and global information infrastructure is essential to promote economic growth, protect privacy, and meet the needs of American citizens and businesses;

(3) the rights of Americans to the privacy and security of their communications and in the conducting of personal and business affairs should be promoted and protected;

(4) the authority and ability of investigative and law enforcement officers to access and decipher, in a timely manner and as provided by law, wire and electronic communications, and stored electronic information necessary to provide for public safety and national security should also be preserved;

(5) individuals will not entrust their sensitive personal, medical, financial, and other information to computers and computer networks unless the security and privacy of that information is assured;

(6) businesses will not entrust their proprietary and sensitive corporate information, including information about products, processes, customers, finances, and employees, to computers and computer networks unless the security and privacy of that information is assured;

(7) America's critical infrastructures, including its telecommunications system, banking and financial infrastructure, and power and transportation infrastructure, increasingly rely on vulnerable information systems, and will represent a growing risk to national security and public safety unless the security and privacy of those information systems is assured;

(8) encryption technology is an essential tool to promote and protect the privacy, security, confidentiality, integrity, and authenticity of wire and electronic communications and stored electronic information;

(9) encryption techniques, technology, programs, and products are widely available worldwide;

(10) Americans should be free to use lawfully whatever particular encryption techniques, technologies, programs, or products developed in the marketplace that best suits their needs in order to interact electronically with the government and others worldwide in a secure, private, and confidential manner;

(11) government mandates for, or otherwise compelled use of, third-party key recovery systems or other systems that provide surreptitious access to encrypted data threatens the security and privacy of information systems;

(12) American companies should be free to compete and sell encryption technology, programs, and products, and to exchange encryption technology, programs, and products through the use of the Internet, which is rapidly emerging as the preferred method of distribution of computer software and related information;

(13) a national encryption policy is needed to advance the development of the national and global information infrastructure, and preserve the right to privacy of Americans and the public safety and national security of the United States;

(14) Congress and the American people have recognized the need to balance the right to privacy and the protection of the public safety with national security;

(15) the Constitution of the United States permits lawful electronic surveillance by investigative or law enforcement officers and the seizure of stored electronic information only upon compliance with stringent standards and procedures; and

(16) there is a need to clarify the standards and procedures by which investigative or law enforcement officers obtain decryption assistance from persons—

(A) who are voluntarily entrusted with the means to decrypt wire and electronic communications and stored electronic information; or

(B) have information that enables the decryption of such communications and information.

SEC. 4. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 6 of title 18, United States Code.

(2) COMPUTER HARDWARE.—The term ''computer hardware'' includes computer systems, equipment, application-specific assemblies, smart cards, modules, and integrated circuits.

(3) COMPUTING DEVICE.—The term ''computing device'' means a device that incorporates 1 or more microprocessor-based central processing units that are capable of accepting, storing, processing, or providing output of data.

(4) ENCRYPT AND ENCRYPTION.—The terms ''encrypt'' and ''encryption'' refer to the scrambling (and descrambling) of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information.

(5) ENCRYPTION PRODUCT.—The term ''encryption product''—

(A) means a computing device, computer hardware, computer software, or technology, with encryption capabilities; and

(B) includes any subsequent version of or update to an encryption product, if the encryption capabilities are not changed.

(6) EXPORTABLE.—The term ''exportable'' means the ability to transfer, ship, or transmit to foreign users.

(7) KEY.—The term ''key'' means the variable information used in or produced by a mathematical formula, code, or algorithm, or any component thereof, used to encrypt or decrypt wire communications, electronic communications, or electronically stored information.

(8) PERSON.—The term ''person'' has the meaning given the term in section 2510(6) of title 18, United States Code.

(9) REMOTE COMPUTING SERVICE.—The term ''remote computing service'' has the meaning given the term in section 2711(2) of title 18, United States Code.

(10) STATE.—The term ''State'' has the meaning given the term in section 3156(a)(5) of title 18, United States Code.

(11) TECHNICAL REVIEW.—The term ''technical review'' means a review by the Secretary, based on information about a product's encryption capabilities supplied by the manufacturer, that an encryption product works as represented.

(12) UNITED STATES PERSON.—The term ''United States person'' means any—

(A) United States citizen; or

(B) any legal entity that—

(i) is organized under the laws of the United States, or any State, the District of Columbia, or any commonwealth, territory, or possession of the United States; and

(ii) has its principal place of business in the United States.

TITLE I—PRIVACY PROTECTION FOR COMMUNICATIONS AND ELECTRONIC INFORMATION

SEC. 101. FREEDOM TO USE ENCRYPTION.

(a) IN GENERAL.—Except as otherwise provided by this Act and the amendments made by this Act, it shall be lawful for any person within the United States, and for any United States person in a foreign country, to use, develop, manufacture, sell, distribute, or import any encryption product, regardless of the encryption algorithm selected, encryption key length chosen, existence of key recovery or other plaintext access capability, or implementation or medium used.

(b) PROHIBITION ON GOVERNMENT-COMPELLED KEY ESCROW OR KEY RECOVERY ENCRYPTION.—

(1) IN GENERAL.—Except as provided in paragraph (3), no agency of the United States nor any State may require, compel, set standards for, condition any approval on, or condition the receipt of any benefit on, a requirement that a decryption key, access to a decryption key, key recovery information, or other plaintext access capability be—

(A) given to any other person, including any agency of the United States or a State, or any entity in the private sector; or

(B) retained by any person using encryption.

(2) USE OF PARTICULAR PRODUCTS.—No agency of the United States may require any person who is not an employee or agent of the United States or a State to use any key recovery or other plaintext access features for communicating or transacting business with any agency of the United States.

(3) EXCEPTION.—The prohibition in paragraph (1) does not apply to encryption used by an agency of the United States or a State, or the employees or agents of such an agency, solely for the internal operations and telecommunications systems of the United States or the State.

(c) USE OF ENCRYPTION FOR AUTHENTICATION OR INTEGRITY PURPOSES.—

(1) IN GENERAL.—The use, development, manufacture, sale, distribution and import of encryption products, standards, and services for purposes of assuring the confidentiality, authenticity, or integrity or access control of electronic information shall be voluntary and market driven.

(2) CONDITIONS.—No agency of the United States or a State shall establish any condition, tie, or link between encryption products, standards, and services used for confidentiality, and those used for authentication, integrity, or access control purposes.

SEC. 102. PURCHASE AND USE OF ENCRYPTION PRODUCTS BY THE FEDERAL GOVERNMENT.

(a) PURCHASES.—An agency of the United States may purchase encryption products for—

(1) the internal operations and telecommunications systems of the agency; or

(2) use by, among, and between that agency and any other agency of the United States, the employees of the agency, or persons operating under contract with the agency.

(b) INTEROPERABILITY.—To ensure that secure electronic access to the Government is

available to persons outside of and not operating under contract with agencies of the United States, the United States shall purchase no encryption product with a key recovery or other plaintext access feature if such key recovery or plaintext access feature would interfere with use of the product's full encryption capabilities when interoperating with other commercial encryption products.

SEC. 103. ENHANCED PRIVACY PROTECTION FOR INFORMATION ON COMPUTER NETWORKS.

Section 2703 of title 18, United States Code, is amended by adding at the end the following:

''(g) ACCESS TO STORED ELECTRONIC INFORMATION.—

''(1) DISCLOSURE.—

''(A) IN GENERAL.—Subject to subparagraph (B), a governmental entity may require the disclosure by a provider of a remote computing service of the contents of an electronic record in networked electronic storage only if the person who created the record is accorded the same protections that would be available if the record had remained in that person's possession.

''(B) NETWORKED ELECTRONIC STORAGE.—In addition to the requirements of subparagraph (A) and subject to paragraph (2), a governmental entity may require the disclosure of the contents of an electronic record in networked electronic storage only—

''(i) pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant, a copy of which warrant shall be served on the person who created the record prior to or at the same time the warrant is served on the provider of the remote computing service;

''(ii) pursuant to a subpoena issued under the Federal Rules of Criminal Procedure or equivalent State warrant, a copy of which subpoena shall be served on the person who created the record, under circumstances allowing that person a meaningful opportunity to challenge the subpoena; or

''(iii) upon the consent of the person who created the record.

''(2) DEFINITION.—In this subsection, an electronic record is in 'networked electronic storage' if—

''(A) it is not covered by subsection (a) of this section;

''(B) the person holding the record is not authorized to access the contents of such record for any purposes other than in connection with providing the service of storage; and

''(C) the person who created the record is able to access and modify it remotely through electronic means.''.

SEC. 104. GOVERNMENT ACCESS TO LOCATION INFORMATION.

(a) COURT ORDER REQUIRED.—Section 2703 of title 18, United States Code, is amended by adding at the end the following:

''(h) REQUIREMENTS FOR DISCLOSURE OF LOCATION INFORMATION.—A provider of mobile electronic communication service shall provide to a governmental entity information generated by and disclosing, on a real time basis, the physical location of a subscriber's equipment only if the governmental entity obtains a court order issued upon a finding that there is probable cause to believe that an individual using or possessing the subscriber equipment is committing, has committed, or is about to commit a felony offense.''.

(b) CONFORMING AMENDMENT.—Section 2703(c)(1)(B) of title 18, United States Code, is amended by inserting ''or wireless location information covered by subsection (g) of this section'' after ''(b) of this section''.

SEC. 105. ENHANCED PRIVACY PROTECTION FOR TRANSACTIONAL INFORMATION OBTAINED FROM PEN REGISTERS OR TRAP AND TRACE DEVICES.

Subsection 3123(a) of title 18, United States Code, is amended to read as follows:

''(a) IN GENERAL.—Upon an application made under section 3122, the court may enter an ex parte order—

''(1) authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds, based on the certification by the attorney for the Government or the State law enforcement or investigative officer, that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation; and

''(2) directing that the use of the pen register or trap and trace device be conducted in such a way as to minimize the recording or decoding of any electronic or other impulses that are not related to the dialing and signaling information utilized in call processing.''.

TITLE II—LAW ENFORCEMENT ASSISTANCE

SEC. 201. ENCRYPTED WIRE OR ELECTRONIC COMMUNICATIONS AND STORED ELECTRONIC COMMUNICATIONS.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by inserting after chapter 123 the following:

''CHAPTER 124—ENCRYPTED WIRE OR ELECTRONIC COMMUNICATIONS AND STORED ELECTRONIC INFORMATION

''Sec.
''2801. Definitions.
''2802. Unlawful use of encryption.
''2803. Access to decryption assistance for communications.
''2804. Access to decryption assistance for stored electronic communications or records.
''2805. Foreign government access to decryption assistance.
''2806. Establishment and operations of National Electronic Technologies Center.

''§ 2801. Definitions

''In this chapter:

''(1) DECRYPTION ASSISTANCE.—The term 'decryption assistance' means assistance that provides or facilitates access to the plaintext of an encrypted wire or electronic communication or stored electronic information, including the disclosure of a decryption key or the use of a decryption key to produce plaintext.

''(2) DECRYPTION KEY.—The term 'decryption key' means the variable information used in or produced by a mathematical formula, code, or algorithm, or any component thereof, used to decrypt a wire communication or electronic communication or stored electronic information that has been encrypted.

''(3) ENCRYPT; ENCRYPTION.—The terms 'encrypt' and 'encryption' refer to the scrambling (and descrambling) of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information.

''(4) FOREIGN GOVERNMENT.—The term 'foreign government' has the meaning given the term in section 1116.

''(5) OFFICIAL REQUEST.—The term 'official request' has the meaning given the term in section 3506(c).

''(6) INCORPORATED DEFINITIONS.—Any term used in this chapter that is not defined in this chapter and that is defined in section 2510, has the meaning given the term in section 2510.

''§ 2802. Unlawful use of encryption

''Any person who, during the commission of a felony under Federal law, knowingly and willfully encrypts any incriminating communication or information relating to that felony, with the intent to conceal that communication or information for the purpose of avoiding detection by a law enforcement agency or prosecutor—

''(1) in the case of a first offense under this section, shall be imprisoned not more than 5 years, fined under this title, or both; and

''(2) in the case of a second or subsequent offense under this section, shall be imprisoned not more than 10 years, fined under this title, or both.

''§ 2803. Access to decryption assistance for communications

''(a) CRIMINAL INVESTIGATIONS.—

''(1) IN GENERAL.—An order authorizing the interception of a wire or electronic communication under section 2518 shall, upon request of the applicant, direct that a provider of wire or electronic communication service, or any other person possessing information capable of decrypting that communication, other than a person whose communications are the subject of the interception, shall promptly furnish the applicant with the necessary decryption assistance, if the court finds that the decryption assistance sought is necessary for the decryption of a communication intercepted pursuant to the order.

''(2) LIMITATIONS.—Each order described in paragraph (1), and any extension of such an order, shall—

''(A) contain a provision that the decryption assistance provided shall involve disclosure of a private key only if no other form of decryption assistance is available and otherwise shall be limited to the minimum necessary to decrypt the communications intercepted pursuant to this chapter; and

''(B) terminate on the earlier of—

''(i) the date on which the authorized objective is attained; or

''(ii) 30 days after the date on which the order or extension, as applicable, is issued.

''(3) NOTICE.—If decryption assistance is provided pursuant to an order under this subsection, the court issuing the order described in paragraph (1)—

''(A) shall cause to be served on the person whose communications are the subject of such decryption assistance, as part of the inventory required to be served pursuant to section 2518(8), notice of the receipt of the decryption assistance and a specific description of the keys or other assistance disclosed; and

''(B) upon the filing of a motion and for good cause shown, shall make available to such person, or to counsel for that person, for inspection, the intercepted communications to which the decryption assistance related, except that on an ex parte showing of good cause, the serving of the inventory required by section 2518(8) may be postponed.

''(b) FOREIGN INTELLIGENCE INVESTIGATIONS.—

''(1) IN GENERAL.—An order authorizing the interception of a wire or electronic communication under section 105(b)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(b)(2)) shall, upon request of the applicant, direct that a provider of wire or electronic communication service or any other person possessing information capable of decrypting such communications, other than a person whose communications are the subject of the interception, shall promptly furnish the applicant with the necessary decryption assistance, if the court finds that

the decryption assistance sought is necessary for the decryption of a communication intercepted pursuant to the order.

''(2) LIMITATIONS.—Each order described in paragraph (1), and any extension of such an order, shall—

''(A) contain a provision that the decryption assistance provided shall be limited to the minimum necessary to decrypt the communications intercepted pursuant to this chapter; and

''(B) terminate on the earlier of—

''(i) the date on which the authorized objective is attained; or

''(ii) 30 days after the date on which the order or extension, as applicable, is issued.

''(c) GENERAL PROHIBITION ON DISCLOSURE.—Other than pursuant to an order under subsection (a) or (b) of this section, no person possessing information capable of decrypting a wire or electronic communication of another person shall disclose that information or provide decryption assistance to an investigative or law enforcement officer (as defined in section 2510(7)).

''§ 2804. Access to decryption assistance for stored electronic communications or records

''(a) DECRYPTION ASSISTANCE.—No person may disclose a decryption key or provide decryption assistance pertaining to the contents of stored electronic communications or records, including those disclosed pursuant to section 2703, to a governmental entity, except—

''(1) pursuant to a warrant issued under the Federal Rules of Criminal Procedure or an equivalent State warrant, a copy of which warrant shall be served on the person who created the electronic communication prior to or at the same time service is made on the keyholder;

''(2) pursuant to a subpoena, a copy of which subpoena shall be served on the person who created the electronic communication or record, under circumstances allowing the person meaningful opportunity to challenge the subpoena; or

''(3) upon the consent of the person who created the electronic communication or record.

''(b) DELAY OF NOTIFICATION.—In the case of communications disclosed pursuant to section 2703(a), service of the copy of the warrant or subpoena on the person who created the electronic communication under subsection (a) may be delayed for a period of not to exceed 90 days upon request to the court by the governmental entity requiring the decryption assistance, if the court determines that there is reason to believe that notification of the existence of the court order or subpoena may have an adverse result described in section 2705(a)(2).

''§ 2805. Foreign government access to decryption assistance

''(a) IN GENERAL.—No investigative or law enforcement officer may—

''(1) release a decryption key to a foreign government or to a law enforcement agency of a foreign government; or

''(2) except as provided in subsection (b), provide decryption assistance to a foreign government or to a law enforcement agency of a foreign government.

''(b) CONDITIONS FOR COOPERATION WITH FOREIGN GOVERNMENT.—

''(1) APPLICATION FOR AN ORDER.—In any case in which the United States has entered into a treaty or convention with a foreign government to provide mutual assistance with respect to providing decryption assistance, the Attorney General (or the designee of the Attorney General) may, upon an official request to the United States from the foreign government, apply for an order described in paragraph (2) from the district court in which the person possessing information capable of decrypting the communication or information at issue resides—

''(A) directing that person to release a decryption key or provide decryption assistance to the Attorney General (or the designee of the Attorney General); and

''(B) authorizing the Attorney General (or the designee of the Attorney General) to furnish the foreign government with the plaintext of the encrypted communication or stored electronic information at issue.

''(2) CONTENTS OF ORDER.—An order is described in this paragraph if it is an order directing the person possessing information capable of decrypting the communication or information at issue to

''(A) release a decryption key to the Attorney General (or the designee of the Attorney General) so that the plaintext of the communication or information may be furnished to the foreign government; or

''(B) provide decryption assistance to the Attorney General (or the designee of the Attorney General) so that the plaintext of the communication or information may be furnished to the foreign government.

''(3) REQUIREMENTS FOR ORDER.—The court described in paragraph (1) may issue an order described in paragraph (2) if the court finds, on the basis of an application made by the Attorney General under this subsection, that—

''(A) the decryption key or decryption assistance sought is necessary for the decryption of a communication or information that the foreign government is authorized to intercept or seize pursuant to the law of that foreign country;

''(B) the law of the foreign country provides for adequate protection against arbitrary interference with respect to privacy rights; and

''(C) the decryption key or decryption assistance is being sought in connection with a criminal investigation for conduct that would constitute a violation of a criminal law of the United States if committed within the jurisdiction of the United States.

''§ 2806. Establishment and operations of National Electronic Technologies Center

''(a) NATIONAL ELECTRONIC TECHNOLOGIES CENTER.—

''(1) ESTABLISHMENT.—There is established in the Department of Justice a National Electronic Technologies Center (referred to in this section as the 'NET Center').

''(2) DIRECTOR.—The NET Center shall be administered by a Director (referred to in this section as the 'Director'), who shall be appointed by the Attorney General.

''(3) DUTIES.—The NET Center shall—

''(A) serve as a center for Federal, State, and local law enforcement authorities for information and assistance regarding decryption and other access requirements;

''(B) serve as a center for industry and government entities to exchange information and methodology regarding information security techniques and technologies;

''(C) support and share information and methodology regarding information security techniques and technologies with the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) and Field Computer Investigations and Infrastructure Threat Assessment (CITA) Squads of the Federal Bureau of Investigation;

''(D) examine encryption techniques and methods to facilitate the ability of law enforcement to gain efficient access to plaintext of communications and electronic information;

''(E) conduct research to develop efficient methods, and improve the efficiency of existing methods, of accessing plaintext of communications and electronic information;

''(F) investigate and research new and emerging techniques and technologies to facilitate access to communications and electronic information, including—

''(i) reverse-stenography;

''(ii) decompression of information that previously has been compressed for transmission; and

''(iii) demultiplexing;

''(G) investigate and research interception and access techniques that preserve the privacy and security of information not authorized to be intercepted; and

''(H) obtain information regarding the most current hardware, software, telecommunications, and other capabilities to understand how to access digitized information transmitted across networks.

''(4) EQUAL ACCESS.—State and local law enforcement agencies and authorities shall have access to information, services, resources, and assistance provided by the NET Center to the same extent that Federal law enforcement agencies and authorities have such access.

''(5) PERSONNEL.—The Director may appoint such personnel as the Director considers appropriate to carry out the duties of the NET Center.

''(6) ASSISTANCE OF OTHER FEDERAL AGENCIES.—Upon the request of the Director of the NET Center, the head of any department or agency of the Federal Government may, to assist the NET Center in carrying out its duties under this subsection—

''(A) detail, on a reimbursable basis, any of the personnel of such department or agency to the NET Center; and

''(B) provide to the NET Center facilities, information, and other nonpersonnel resources.

''(7) PRIVATE INDUSTRY ASSISTANCE.—The NET Center may accept, use, and dispose of gifts, bequests, or devises of money, services, or property, both real and personal, for the purpose of aiding or facilitating the work of the Center. Gifts, bequests, or devises of money and proceeds from sales of other property received as gifts, bequests, or devises shall be deposited in the Treasury and shall be available for disbursement upon order of the Director of the NET Center.

''(8) ADVISORY BOARD.—

''(A) ESTABLISHMENT.—There is established in the NET Center an Advisory Board for Excellence in Information Security (in this paragraph referred to as the 'Advisory Board'), which shall be comprised of members who have the qualifications described in subparagraph (B) and who are appointed by the Attorney General. The Attorney General shall appoint a chairman of the Advisory Board.

''(B) QUALIFICATIONS.—Each member of the Advisory Board shall have experience or expertise in the field of encryption, decryption, electronic communication, information security, electronic commerce, privacy protection, or law enforcement.

''(C) DUTIES.—The duty of the Advisory Board shall be to advise the NET Center and the Federal Government regarding new and emerging technologies relating to encryption and decryption of communications and electronic information.

''(9) IMPLEMENTATION PLAN.—

''(A) IN GENERAL.—Not later than 2 months after the date of enactment of this chapter, the Attorney General shall, in consultation and cooperation with other appropriate Federal agencies and appropriate industry participants, develop and cause to be published in the Federal Register a plan for establishing the NET Center.

''(B) CONTENTS OF PLAN.—The plan published under subparagraph (A) shall—

''(i) specify the physical location of the NET Center and the equipment, software,

and personnel resources necessary to carry out the duties of the NET Center under this subsection;

''(ii) assess the amount of funding necessary to establish and operate the NET Center; and

''(iii) identify sources of probable funding for the NET Center, including any sources of in-kind contributions from private industry.

''(b) AUTHORIZATION.—There are authorized to be appropriated such sums as may be necessary for the establishment and operation of the NET Center.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The analysis for part I of title 18, United States Code, is amended by adding at the end the following:

''124. Encrypted wire or electronic communications and stored electronic information ..... 2801''.

TITLE III—EXPORTS OF ENCRYPTION PRODUCTS

SEC. 301. COMMERCIAL ENCRYPTION PRODUCTS.

(a) PROVISIONS APPLICABLE TO COMMERCIAL PRODUCTS.—The provisions of this title apply to all encryption products, regardless of the encryption algorithm selected, encryption key length chosen, exclusion of key recovery or other plaintext access capability, or implementation or medium used, except those specifically designed or modified for military use, including command, control, and intelligence applications.

(b) CONTROL BY SECRETARY OF COMMERCE.—Subject to the provisions of this title, and notwithstanding any other provision of law, the Secretary of Commerce shall have exclusive authority to control exports of encryption products covered under subsection (a).

SEC. 302. LICENSE EXCEPTION FOR MASS MARKET PRODUCTS.

(a) EXPORT CONTROL RELIEF.—Subject to section 307, an encryption product that is generally available, or incorporates or employs in any form, implementation, or medium, an encryption product that is generally available, shall be exportable without the need for an export license, and without restrictions other than those permitted under this Act, after a 1-time 15-day technical review by the Secretary of Commerce.

(b) DEFINITIONS.—In this section, the term ''generally available'' means an encryption product that is—

(1) offered for sale, license, or transfer to any person without restriction, whether or not for consideration, including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval; and

(2) not designed, developed, or customized by the manufacturer for specific purchasers except for user or purchaser selection among installation or configuration parameters.

(c) COMMERCE DEPARTMENT ASSURANCE.—

(1) IN GENERAL.—The manufacturer or exporter of an encryption product may request written assurance from the Secretary of Commerce that an encryption product is considered generally available for purposes of this section.

(2) RESPONSE.—Not later than 30 days after receiving a request under paragraph (1), the Secretary shall make a determination regarding whether to issue a written assurance under that paragraph, and shall notify the person making the request, in writing, of that determination.

(3) EFFECT ON MANUFACTURERS AND EXPORTERS.—A manufacturer or exporter who obtains a written assurance under this subsection shall not be held liable, responsible, or subject to sanctions for failing to obtain an export license for the encryption product at issue.

SEC. 303. LICENSE EXCEPTION FOR PRODUCTS WITHOUT ENCRYPTION CAPABLE OF WORKING WITH ENCRYPTION PRODUCTS.

Subject to section 307, any product that does not itself provide encryption capabilities, but that incorporates or employs in any form cryptographic application programming interfaces or other interface mechanisms for interaction with other encryption products covered by section 301(a), shall be exportable without the need for an export license, and without restrictions other than those permitted under this Act, after a 1-time, 15-day technical review by the Secretary of Commerce.

SEC. 304. LICENSE EXCEPTION FOR PRODUCT SUPPORT AND CONSULTING SERVICES.

(a) NO ADDITIONAL EXPORT CONTROLS IMPOSED IF UNDERLYING PRODUCT COVERED BY LICENSE EXCEPTION.—Technical assistance and technical data associated with the installation and maintenance of encryption products covered by sections 302 and 303 shall be exportable without the need for an export license, and without restrictions other than those permitted under this Act.

(b) DEFINITIONS.—In this section:

(1) TECHNICAL ASSISTANCE.—The term ''technical assistance'' means services, including instruction, skills training, working knowledge, and consulting services, and the transfer of technical data.

(2) TECHNICAL DATA.—The term ''technical data'' means information including blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, or read-only memories.

SEC. 305. LICENSE EXCEPTION WHEN COMPARABLE FOREIGN PRODUCTS AVAILABLE.

(a) FOREIGN AVAILABILITY STANDARD.—An encryption product not qualifying under section 302 shall be exportable without the need for an export license, and without restrictions other than those permitted under this Act, after a 1-time 15-day technical review by the Secretary of Commerce, if an encryption product utilizing the same or greater key length or otherwise providing comparable security to such encryption product is, or will be within the next 18 months, commercially available outside the United States from a foreign supplier.

(b) DETERMINATION OF FOREIGN AVAILABILITY.—

(1) ENCRYPTION EXPORT ADVISORY BOARD ESTABLISHED.—There is hereby established a board to be known as the ''Encryption Export Advisory Board'' (in this section referred to as the ''Board'').

(2) MEMBERSHIP.—The Board shall be comprised of—

(A) the Under Secretary of Commerce for Export Administration, who shall be Chairman;

(B) seven individuals appointed by the President, of whom—

(i) one shall be a representative from each of—

(I) the National Security Agency;

(II) the Central Intelligence Agency; and

(III) the Office of the President; and

(ii) four shall be individuals from the private sector who have expertise in the development, operation, or marketing of information technology products; and

(C) four individuals appointed by Congress from among individuals in the private sector who have expertise in the development, operation, or marketing of information technology products, of whom—

(i) one shall be appointed by the Majority Leader of the Senate;

(ii) one shall be appointed by the Minority Leader of the Senate;

(iii) one shall be appointed by the Speaker of the House of Representatives; and

(iv) one shall be appointed by the Minority Leader of the House of Representatives.

(3) MEETINGS.—

(A) IN GENERAL.—Subject to subparagraph (B), the Board shall meet at the call of the Under Secretary of Commerce for Export Administration.

(B) MEETINGS WHEN APPLICATIONS PENDING.—If any application referred to in paragraph (4)(A) is pending, the Board shall meet not less than once every 30 days.

(4) DUTIES.—

(A) IN GENERAL.—Whenever an application for a license exception for an encryption product under this section is submitted to the Secretary of Commerce, the Board shall determine whether a comparable encryption product is commercially available outside the United States from a foreign supplier as specified in subsection (a).

(B) MAJORITY VOTE REQUIRED.—The Board shall make a determination under this paragraph upon a vote of the majority of the members of the Board.

(C) DEADLINE.—The Board shall make a determination with respect to an encryption product under this paragraph not later than 30 days after receipt by the Secretary of an application for a license exception under this subsection based on the encryption product.

(D) NOTICE OF DETERMINATIONS.—The Board shall notify the Secretary of Commerce of each determination under this paragraph.

(E) REPORTS TO PRESIDENT.—Not later than 30 days after a meeting under this paragraph, the Board shall submit to the President a report on the meeting.

(F) APPLICABILITY OF FACA.—The provisions of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Board or to meetings held by the Board under this paragraph.

(5) ACTION BY SECRETARY OF COMMERCE.—

(A) APPROVAL OR DISAPPROVAL.—The Secretary of Commerce shall specifically approve or disapprove each determination of the Board under paragraph (5) not later than 30 days of the submittal of such determination to the Secretary under that paragraph.

(B) NOTIFICATION AND PUBLICATION OF DECISION.—The Secretary of Commerce shall—

(i) notify the Board of each approval or disapproval under this paragraph; and

(ii) publish a notice of the approval or disapproval in the Federal Register.

(C) CONTENTS OF NOTICE.—Each notice of a decision of disapproval by the Secretary of Commerce under subparagraph (B) of a determination of the Board under paragraph (4) that an encryption product is commercially available outside the United States from a foreign supplier shall set forth an explanation in detail of the reasons for the decision, including why and how continued export control of the encryption product which the determination concerned will be effective in achieving its purpose and the amount of lost sales and loss in market share of United States encryption products as a result of the decision.

(6) JUDICIAL REVIEW.—Notwithstanding any other provision of law, a decision of disapproval by the Secretary of Commerce under paragraph (5) of a determination of the Board under paragraph (4) that an encryption product is commercially available outside the United States from a foreign supplier shall be subject to judicial review under the provisions of subchapter II of chapter 5 of title 5, United States Code (commonly referred to as the ''Administrative Procedures Act'').

(c) INCLUSION OF COMPARABLE FOREIGN ENCRYPTION PRODUCT IN A UNITED STATES PRODUCT NOT BASIS FOR EXPORT CONTROLS.—A product that incorporates or employs a

foreign encryption product, in the way it was intended to be used and that the Board has determined to be commercially available outside the United States, shall be exportable without the need for an export license and without restrictions other than those permitted under this Act, after a 1-time 15-day technical review by the Secretary of Commerce.

SEC. 306. NO EXPORT CONTROLS ON ENCRYPTION PRODUCTS USED FOR NONCONFIDENTIALITY PURPOSES.

(a) PROHIBITION ON NEW CONTROLS.—The Federal Government shall not restrict the export of encryption products used for nonconfidentiality purposes such as authentication, integrity, digital signatures, nonrepudiation, and copy protection.

(b) NO REINSTATEMENT OF CONTROLS ON PREVIOUSLY DECONTROLLED PRODUCTS.—Those encryption products previously decontrolled and not requiring an export license as of January 1, 1998, as a result of administrative decision or rulemaking shall not require an export license.

SEC. 307. APPLICABILITY OF GENERAL EXPORT CONTROLS.

(a) SUBJECT TO TERRORIST AND EMBARGO CONTROLS.—Nothing in this Act shall be construed to limit the authority of the President under the International Emergency Economic Powers Act, the Trading with the Enemy Act, or the Export Administration Act, to—

(1) prohibit the export of encryption products to countries that have been determined to repeatedly provide support for acts of international terrorism; or

(2) impose an embargo on exports to, and imports from, a specific country.

(b) SUBJECT TO SPECIFIC DENIALS FOR SPECIFIC REASONS.—The Secretary of Commerce shall prohibit the export of particular encryption products to an individual or organization in a specific foreign country identified by the Secretary if the Secretary determines that there is substantial evidence that such encryption products will be used for military or terrorist end-use, including acts against the national security, public safety, or the integrity of the transportation, communications, or other essential systems of interstate commerce in the United States.

(c) OTHER EXPORT CONTROLS REMAIN APPLICABLE.—(1) Encryption products shall remain subject to all export controls imposed on such products for reasons other than the existence of encryption capabilities.

(2) Nothing in this Act alters the Secretary's ability to control exports of products for reasons other than encryption.

SEC. 308. FOREIGN TRADE BARRIERS TO UNITED STATES PRODUCTS.

Not later than 180 days after the date of enactment of this Act, the Secretary of Commerce, in consultation with the United States Trade Representative, shall—

(1) identify foreign barriers to exports of United States encryption products;

(2) initiate appropriate actions to address such barriers; and

(3) submit to Congress a report on the actions taken under this section.

Mr. LEAHY. Mr. President, I am pleased to join Senator ASHCROFT, and others, in introducing today the ''Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace,'' or E-PRIVACY Act, to reform our nation's cryptography policy in a constructive and positive manner. It is time the Administration woke up to the critical need for a common sense encryption policy in this country.

I have been sounding the alarm bells about this issue for several years now, and have introduced encryption legislation, with bipartisan support, in the last Congress and again in this one, to balance the important privacy, economic, national security and law enforcement interests at stake. The volume of those alarm bells should be raised to emergency sirens.

Hardly a month goes by without press reports of serious breaches of computer security that threaten our critical infrastructures, including Defense Department computer systems, the telephone network, or computer systems for airport control towers. The lesson of these computer breaches—often committed by computer savvy teenagers—is that all the physical barriers we might put in place can be circumvented using the wires that run into every building to support the computers and computer networks that are the mainstay of how we do business. A well-focused cyber-attack on the computer networks that support telecommunications, transportation, water supply, banking, electrical power and other critical infrastructure systems could wreak havoc on our national economy or even jeopardize our national defense or public safety.

We have been aware of the vulnerabilities of our computer networks for some time. It became clear to me almost a decade ago, during hearings I chaired of the Judiciary Subcommittee on Technology and the Law on the risks of high-tech terrorism, that merely ''hardening'' our physical space from potential attack is not enough. We must also ''harden'' our critical infrastructures to ensure our security and our safety.

That is where encryption technology comes in. Encryption can protect the security of our computer information and networks. Indeed, both former Senator Sam Nunn and former Deputy Attorney General Jamie Gorelick, who serve as co-chairs of the Advisory Committee to the President's Commission on Critical Infrastructure Protection, have testified that ''encryption is essential for infrastructure protection.''

Yet U.S. encryption policy has acted as a deterrent to better security. As long ago as 1988, at the High-Tech Terrorism hearings I chaired, Jim Woolsey, who later became the director of the Central Intelligence Agency, testified about the need to do a better job of using encryption to protect our computer networks. Of particular concern is the recent testimony of former Senator Sam Nunn that the ''continuing federal government-private sector deadlock over encryption and export policies'' may pose an obstacle to the cooperation needed to protect our country's critical infrastructures.

I have long advocated the use of strong encryption by individuals, government agencies and private companies to protect their valuable and confidential computer information. Moreover, as more Americans every year use the Internet and other computer networks to obtain critical medical services, and conduct their personal and business affairs, maintaining the privacy and confidentiality of our computer communications both here and abroad has only grown in importance. As an avid computer user and Internet surfer myself, I care deeply about protecting individual privacy and encouraging the development of the Internet as a secure and trusted communications medium.

Encryption is the key to protecting the privacy of our online communications and electronic records by ensuring that only the people we choose can read those communications and records. That is why the primary thrust of the encryption legislation I have introduced is to encourage—and not stand in the way of—the widespread use of strong encryption.

Strong encryption serves as a crime prevention shield to stop hackers, industrial spies and thieves from snooping into private computer files and stealing valuable proprietary information. Unfortunately, we still have a long away to go to reform our country's encryption policy to reflect that this technology is a significant crime and terrorism prevention tool.

Even as our law enforcement and intelligence agencies try to slow down the widespread use of strong encryption, technology continues to move forward. Ironically, foot-dragging by the Administration on export controls is driving encryption technology, expertise and manufacturing overseas where we will lose even more control over its proliferation.

Indeed, due to the sorry state of our export controls on encryption, we are seeing rising numbers of our high-tech companies turning to overseas firms as suppliers of the strong encryption demanded by their customers. For example, Network Associates recently announced that it will make strong encryption software developed in the United States available through a Swiss company. Other companies, including Sun Microsystems, are cooperating with foreign firms to manufacture and distribute overseas strong encryption software originally developed here at home.

Encryption technology, invented with American ingenuity, will now be manufactured and distributed in Europe, and imported back into this country.

Driving encryption expertise overseas is extremely short-sighted and poses a real threat to our national security. Driving high-tech jobs overseas is a threat to our economic security, and stifling the widespread, integrated use of strong encryption is a threat to our public safety. The E-PRIVACY Act would reverse the incentives for American companies to look abroad for strong encryption by relaxing our export controls.

Specifically, the bill would grant export license exceptions, after a one-time technical review, for mass market products with encryption capabilities,

products which do not themselves provide encryption but are capable of interoperating with encryption products, and customized hardware and software with encryption capabilities so long as foreign products with comparable encryption are available.

At the same time, the bill retains important restrictions on encryption exports for military end-uses or to terrorist-designated or embargoed countries, such as Cuba and North Korea. It also affirms the continued authority of the Secretary of Commerce over encryption exports and assures that before export, the Secretary is able to conduct a one-time technical review of all encryption products to ensure that the product works as represented.

The E-PRIVACY Act puts to rest the specter of domestic controls on encryption. This legislation bars government-mandated key recovery (or key escrow encryption) and ensures that all computer users are free to choose any encryption method to protect the privacy of their online communications and computer files.

At the heart of the encryption debate is the power this technology gives computer users to choose who may access their communications and stored records, to the exclusion of all others. For the same reason that encryption is a powerful privacy enhancing tool, it also poses challenges for law enforcement. Law enforcement agencies want access even when we do not choose to give it. We are mindful of these national security and law enforcement concerns that have dictated the Administration's policy choices on encryption.

With the appropriate procedural safeguards in place, law enforcement agencies should be able to get access to decryption assistance. The E-PRIVACY Act contains a number of provisions designed to address these concerns, including a new criminal offense for willful use of encryption to hide incriminating evidence from law enforcement detection, establishment of a NET Center to help federal, state and local law enforcement stay abreast of advanced technologies, and explicit procedures for law enforcement to obtain decryption assistance from third parties for encrypted communications or records to which law enforcement has lawful access.

One of the starkest deficiencies in the Administration's key recovery proposals has always been the question of foreign government access. The Administration has sought reciprocal relationships with foreign governments as a critical part of an effective global key recovery system. Yet many Americans and American companies are rightfully concerned about the terms under which foreign governments would get access to decryption assistance. The E-PRIVACY Act makes clear what those terms will be and ensures that foreign governments will not get access to private decryption keys, but only, at most, plaintext.

This is not just an important issue for the privacy and security of Americans; it also is a significant human rights issue. Today, human rights organizations worldwide are using encryption to protect their work and the lives of investigators, witnesses and victims overseas. Amnesty International uses it. Human Rights Watch uses it. The human rights program in the American Association for the Advancement of Science uses it. It is used to protect witnesses who report human rights abuses in the Balkans, in Burma, in Guatemala, in Tibet. I have been told about a number of other instances in which strong encryption has been used to further the causes of democracy and human rights.

For example, in the ongoing trial of Argentinean military officers in Spain, on charges of genocide and terrorism arising out of the ''dirty war,'' the human rights group Derechos uses the encryption program Pretty Good Privacy (PGP)—which the United States government tried to keep out of the hands of foreigners—to encrypt particularly confidential messages that go between Spain and Argentina, to stop the Argentinean intelligence forces from being able to read them and so try to jeopardize the trial.

A group in Guatemala is using a computer database to track the names of witnesses to military massacres. A South African organization keeps the names of applicants for amnesty for political crimes carried out in South Africa during the apartheid regime. Workers at both groups could be subject to intimidation, harassment, or murder by those intent on preventing the public discussion and analysis of the claims. Both systems are protected by strong cryptography.

A not-for-profit agency working for human rights in the Balkans uses PGP to protect all sensitive files. Its offices have been raided by various police forces looking for evidence of ''subversive activities.'' Last year in Zagreb, security police raided its office and confiscated its computers in the hope of retrieving information about the identity of people who had complained about human rights abuses by the authorities. PGP allowed the group to communicate and protect its files from any attempt to gain access. The director of the organization spent 13 days in prison for not opening his encrypted files but has said ''it was a very small price to pay for protecting our clients.''

The Iraqi National Congress, a group opposing Saddam Hussein with offices in London and supporters inside Iraq, uses encrypted e-mail to communicate with its supporters inside Iraq. (Nongovernmental Internet connections are banned in Iraq, but the dissidents within Iraq access e-mail by dialing outside the country with satellite telephones).

Burmese human rights activists working in the relative safe haven of Thailand use encryption when communicating on-line, because the Thai government maintains diplomatic relations with the Burmese government and is expected to turn over information to the Burmese authorities.

The FBI has argued that lives may be lost in sensitive terrorist and other investigations if government agencies do not have access to private encryption keys. However, the reverse is equally true: weak encryption or easy government access to decryption assistance could jeopardize lives as well.

Finally, the E-PRIVACY Act contains provisions to enhance the privacy protections for communications, even when encryption is not employed. Specifically, the bill would require law enforcement to obtain a court order based on probable cause before using a cellular telephone as a tracking device. In addition, the bill would require law enforcement agencies to obtain a court order or provide notice when seizing electronic records that a person stores on a computer network rather than on the hard drive of his or her own personal computer. Finally, the bill grants Federal judges authority to evaluate the reasons proffered by a prosecutor for issuance of an ex parte pen register or trap and trace device order, by contrast to their mere ministerial authority under current law.

In sum, the E-PRIVACY Act accomplishes the eight goals that Senator ASHCROFT and I set out during our April 2, 1998, colloquy on the floor. Specifically, we sought to craft legislation that promotes the following principles:

First, ensure the right of Americans to choose how to protect the privacy and security of their communications and information;

Second, bar a government-mandated key escrow encryption system;

Third, establish both procedures and standards for access by law enforcement to decryption keys or decryption assistance for both encrypted communications and stored electronic information and only permit such access upon court order authorization, with appropriate notice and other procedural safeguards;

Fourth, establish both procedures and standards for access by foreign governments and foreign law enforcement agencies to the plaintext of encrypted communications and stored electronic information of United States persons;

Fifth, modify the current export regime for encryption to promote the global competitiveness of American companies;

Sixth, avoid linking the use of certificate authorities with key recovery agents or, in other words, not link the use of encryption for confidentiality purposes with use of encryption for authenticity and integrity purposes;

Seventh, consistent with these goals of promoting privacy and the global competitiveness of our high-tech industries, help our law enforcement agencies and national security agencies deal with the challenges posed by the use of encryption; and

Eighth, protect the security and privacy of information provided by Americans to the government by ensuring that encryption products used by the government interoperate with commercial encryption products.

Resolving the encryption debate is critical for our economy, our national security and our privacy. This is not a partisan issue. This is not a black-and-white issue of being either for law enforcement and national security or for Internet freedom. Characterizing the debate in these simplistic terms is neither productive nor accurate.

Delays in resolving the encryption debate hurt most the very public safety and national security interests that are posed as obstacles to resolving this issue. We need sensible solutions in legislation that will not be subject to change at the whim of agency bureaucrats.

Every American, not just those in the software and high-tech industries and not just those in law enforcement agencies, has a stake in the outcome of this debate. We have a legislative stalemate right now that needs to be resolved, and I hope to work closely with my colleagues and the Administration on a solution.

I ask unanimous consent that the sectional summary for the ''E-PRIVACY Act'' be printed in the RECORD.

There being no objection, the summary was ordered to be printed in the RECORD, as follows:

SECTION-BY-SECTION ANALYSIS OF E-PRIVACY ACT

SEC. 1. SHORT TITLE.—The Act may be cited as the ''Encryption Protects the Rights of Individuals from Violation and Abuse in CYberspace (E-PRIVACY) Act.''

SEC. 2 Purposes.—The Act would ensure that Americans have the maximum possible choice in encryption methods to protect the security, confidentiality and privacy of their lawful wire and electronic communications and stored electronic information. The Act would also promote the privacy and constitutional rights of individuals and organizations and the security of critical information infrastructures. Finally, the Act would establish privacy standards and procedures for law enforcement officers to follow to obtain decryption assistance for encrypted communications and information.

SEC. 3 FINDINGS.—The Act enumerates sixteen congressional findings, including that a secure, private and trusted national and global information infrastructure is essential to promote citizens' privacy, economic growth and meet the needs of both American citizens and businesses, that encryption technology widely available worldwide can help meet those needs, that Americans should be free to use, and American businesses free to compete and sell, encryption technology, programs and products, and that there is a need to develop a national encryption policy to advance the global information infrastructure and preserve Americans' right to privacy and the Nation's public safety and national security.

SEC. 4 DEFINITIONS.—The terms ''agency'', ''person'', ''remote computing service'' and ''state'' have the same meaning given those terms in specified sections of title 18, United States Code.

Additional definitions are provided for the following terms:

The terms ''encrypt'' and ''encryption'' mean the use of mathematical formulas or algorithms to scramble or descramble electronic data or communications for purposes of confidentiality, integrity, or authenticity. As defined, the terms cover a broad range of scrambling techniques and applications including cryptographic applications such as PGP or RSA's encryption algorithms; stegonagraphy; authentication; and winnowing and chafing.

The term ''encryption product'' includes any hardware, software, devices, or other technology with encryption capabilities, whether or not offered for sale or distribution. A particular encryption product includes subsequent versions of the product, if the encryption capabilities remain the same.

The term ''exportable'' means the ability to transfer, ship, or transmit to foreign users. The term includes the ability to electronically transmit via the Internet.

The term ''key'' means the variable information used in or produced by a mathematical formula to encrypt or decrypt wire or electronic communications, or electronically stored information.

The term ''technical review'' means a review by the Secretary of Commerce based on information about a product's encryption capabilities supplied by the manufacturer that an encryption product works as represented.

TITLE I—PRIVACY PROTECTION FOR COMMUNICATIONS AND ELECTRONIC INFORMATION

SEC. 101. Freedom to use Encryption.

(a) IN GENERAL.—The Act legislatively confirms current practice in the United States that any person in this country may lawfully use any encryption method, regardless of encryption algorithm, key length, existence of key recovery or other plaintext access capability, or implementation selected. Specifically, the Act states the freedom of any person in the U.S., as well as U.S. persons in a foreign country, to make, use, import, and distribute any encryption product without regard to its strength or the use of key recovery, subject to the other provisions of the Act.

(b) PROHIBITION ON GOVERNMENT-COMPELLED KEY ESCROW OR KEY RECOVERY ENCRYPTION.—The Act prohibits any federal or state agency from compelling the use of key recovery systems or other plaintext access systems. Agencies may not set standards, or condition approval or benefits, to compel use of these systems. U.S. agencies may not require persons to use particular key recovery products for interaction with the government. These prohibitions do not apply to systems for use solely for the internal operations and telecommunications systems of a U.S. or a State government agency.

(c) USE OF ENCRYPTION FOR AUTHENTICATION OR INTEGRITY PURPOSES.—The Act requires that the use of encryption products shall be voluntary and market-driven, and no federal or state agency may link the use of encryption for authentication or identity (such as through certificate authority and digital signature systems) to the use of encryption for confidentiality purposes. For example, some Administration proposals would condition receipt of a digital certificate from a licensed certificate authority on the use of key recovery. Such conditions would be prohibited.

SEC. 102. Purchase and Use of Encryption Products by the Federal Government.—The Act authorizes agencies of the United States to purchase encryption products for internal governmental operations and telecommunications systems. To ensure that secure electronic access to the Government is available to persons outside of and not operating under contract with Federal agencies, the Act requires that any key recovery features in encryption products used by the Government interoperate with commercial encryption products.

SEC. 103. Enhanced Privacy Protection For Electronic Records on Computer Networks.—The Act adds a new subsection (g) to section 2703 of title 18, United States Code, to extend privacy protections to electronic information stored on computer networks.

Under *United States* v. *Miller*, 425 U.S. 435 (1976) (customer has no standing to object to bank disclosure of customer records) and its progeny, records in the possession of third parties do not receive Fourth Amendment protection. When held in a person's home, such records can only be seized pursuant to a warrant based upon probable cause, or compelled under a subpoena which can be challenged and quashed. In both these instances, the record owner has notice of the search and an opportunity to challenge it. By contrast, production of records held by third parties can be compelled by a governmental agent with a subpoena to the third party holding the information, without notice to the person to whom the records belong or pertain. The record owner may never receive notice or any meaningful opportunity to challenge the production.

This lack of protection for records held by third parties presents new privacy problems in the information age. With the rise of network computing, electronic information that was previously held on a person's own computer is increasingly stored elsewhere, such as on a network server or an ISP's computers. In many cases the location of such information is not even known to the record's owner.

The Act amends section 2703 to extend the same privacy protections to a person's records whether storage takes place on that person's personal computer in their possession or in networked electronic storage. The term ''networked electronic storage'' applies to electronic records held by a third party, who is not authorized to access the contents of the record except in connection with providing storage services, and where the person who created the record is able to access and modify the record remotely through electronic means. Electronic data stored incident to transmission (such as e-mail) and covered under 2703(a) is not included.

The new section 2703(g) requires that a governmental entity may only require disclosure of electronic records in ''networked electronic storage'' pursuant to (i) a state or federal warrant (based upon probable cause), with a copy to be served on the record owner at the same time the warrant is served on the record holder; (ii) a subpoena that must also be served on the record owner with a meaningful opportunity to challenge the subpoena; or (iii) the consent of the record owner.

SEC. 104. GOVERNMENT ACCESS TO LOCATION INFORMATION.—The Act adds a new subsection (h) to section 2703 of title 18, United States Code, to extend privacy protections for physical location information generated on a real time basis by mobile electronic communications services, such as cellular telephones. This section requires that when cellular telephones are used as contemporaneous tracking devices, the physical location information generated by the service provider may only be released to a governmental entity pursuant to a court order based upon probable cause.

SEC. 105. ENHANCED PRIVACY PROTECTION FOR TRANSACTIONAL INFORMATION OBTAINED FROM PEN REGISTERS OR TRAP AND TRACE DEVICES.—The Act enhances privacy protections for information obtained from pen register and trap and trace devices by amending section 3123(a) of title 18, United States

Code. This amendment would not change the standard for issuance of an ex parte order authorizing use of a pen register or trap and trace device, but would grant a court authority to review the information presented in a certification by the prosecuting attorney to determine whether the information likely to be obtained is relevant to an ongoing criminal investigation. Under current law, the court is relegated to a mere ministerial function and must issue the order upon presentation of a certification.

In addition, the amendment requires law enforcement to minimize the information obtained from the pen register or trap and trace device that is not related to the dialing and signaling information utilized in call processing. Currently, such devices capture not just such dialing information but also any other dialed digits after a call has been completed.

TITLE II—LAW ENFORCEMENT ASSISTANCE

SEC. 201. ENCRYPTED WIRE OR ELECTRONIC COMMUNICATIONS AND STORED ELECTRONIC COMMUNICATIONS.—The Act adds a new chapter 124 to Title 18, Part I, governing the unlawful use of encryption, protections and standards for governmental access, including foreign governments, to decryption assistance from third parties, and establishment of a ''Net Center'' to assist law enforcement in dealing with advanced technologies, such as encryption.

(a) IN GENERAL.—New chapter 124 has six sections. This chapter applies to wire or electronic communications and communications in electronic storage, as defined in 18 U.S.C. §2510, and to stored electronic data. Thus, this chapter describes procedures for law enforcement to obtain assistance in decrypting encrypted electronic mail messages, encrypted telephone conversations, encrypted facsimile transmissions, encrypted computer transmissions and encrypted file transfers over the Internet that are lawfully intercepted pursuant to a wiretap order, under 18 U.S.C. §2518, or obtained pursuant to lawful process, under 18 U.S.C. §2703, and encrypted information stored on computers that are seized pursuant to a search warrant or other lawful process.

§2801. Definitions.—Generally, the terms used in the new chapter have the same meanings as in the federal wiretap statute, 18 U.S.C. §2510. Definitions are provided for ''decryption assistance'', ''decryption key'', ''encrypt; encryption'', ''foreign government'' and ''official request''.

§2802. Unlawful use of encryption.—This section creates a new federal crime for knowingly and willfully using encryption during the commission of a Federal felony offense, with the intent to conceal that information for the purpose of avoiding detection by law enforcement. This new offense would be subject to a fine and up to 5 years' imprisonment for a first offense, and up to 10 years' imprisonment for a second or subsequent offense.

§2803. Access to decryption assistance for communications.—In the United States today, decryption keys and other decryption assistance held by third parties constitute third party records and may be disclosed to a governmental entity with a subpoena or an administrative request, and without any notice to the owner of the encrypted data. Such a low standard of access creates new problems in the information age because encryption users rely heavily on the integrity of keys to protect personal information or sensitive trade secrets, even when those keys are placed in the hands of trusted agents for recovery purposes.

Under new section 2803, in criminal investigations a third party holding decryption keys or other decryption assistance for wire or electronic communications may be required to release such assistance pursuant to a court order, if the court issuing the order finds that such assistance is needed for the decryption of communications covered by the order. Specifically, such an order for decryption assistance may be issued upon a finding that the key or assistance is necessary to decrypt communications or stored data lawfully intercepted or seized. The standard for release of the key or provision of decryption assistance is tied directly to the problem at hand: the need to decrypt a message or information that the government is otherwise authorized to intercept or obtain.

This will ensure that third parties holding decryption keys or decryption information need respond to only one type of compulsory process—a court order. Moreover, this Act will set a single standard for law enforcement, removing any extra burden on law enforcement to demonstrate, for example, probable cause for two separate orders (i.e., for the encrypted communications or information and for decryption assistance) and possibly before two different judges (i.e., the judge issuing the order for the encrypted communications or information and the judge issuing the order to the third party able to provide decryption assistance).

The Act reinforces the principle of minimization. The decryption assistance provided is limited to the minimum necessary to access the particular communications or information specified by court order. Under some key recovery schemes, release of a key holder's private key—rather than an individual session key—might provide the ability to decrypt every communication or stored file ever encrypted by a particular key owner, or by every user in an entire corporation, or by every user who was ever a customer of the key holder. The Act protects against such over broad releases of keys by requiring the court issuing the order to find that the decryption assistance being sought is necessary. Private keys may only be released if no other form of decryption assistance is available.

Notice of the assistance given will be included as part of the inventory provided to subjects of the interception pursuant to current wiretap law standards.

For foreign intelligence investigations, new section 2803 allows FISA orders to direct third-party holders to release decryption assistance if the court finds the assistance is needed to decrypt covered communications. Minimization is also required, though no notice is provided to the target of the investigation.

Under new section 2803, decryption assistance is only required under third-parties (i.e., other than those whose communications are the subject of interception), thereby avoiding self-incrimination problems.

Finally, new section 2803 generally prohibits any person from providing decryption assistance for another person's communications to a governmental entity, except pursuant to the orders described.

§2804. Access to decryption assistance for stored electronic communications or records.—New section 2804 governs access to decryption assistance for stored electronic communications and records.

As noted above, under current law third party decryption assistance may be disclosed to a governmental entity with a subpoena or even a mere request and without notice. This standard is particularly problematic for stored encrypted data, which may exist in insecure media but rely on encryption to maintain security; in such cases easy access to keys destroys the encryption security so heavily relied upon.

Under new section 2804, third parties holding decryption keys or other decryption assistance for stored electronic communications may only release such assistance to a governmental entity pursuant to (1) a state or federal warrant (based upon probable cause), with a copy to be served on the record owner at the same time the warrant is served on the record holder; (2) a subpoena that must also be served on the record owner with a meaningful opportunity to challenge the subpoena; or (3) the consent of the record owner. This standard closely mirrors the protection that would be afforded to encryption keys that are actually kept in the possession of those whose records were encrypted. In the specific case of decryption assistance for communications stored incident to transit (such as e-mail), notice may be delayed under the standards laid out for delayed notice under current law in section 2705(a)(2) of title 18, United States Code.

§2805. Foreign government access to decryption assistance.—New section 2805 creates standards for the U.S. government to provide decryption assistance to foreign governments. No law enforcement officer would be permitted to release decryption keys to a foreign government, but only to provide decryption assistance in the form of producing plaintext. No officer would be permitted to provide decryption assistance except upon an order requested by the Attorney General or designee. Such an order could require the production of decryption keys or assistance to the Attorney General only if the court finds that (1) the assistance is necessary to decrypt data the foreign government is authorized to intercept under foreign law; (2) the foreign country's laws provide ''adequate protection against arbitrary interference with respect to privacy rights''; and (3) the assistance is sought for a criminal investigation of conduct that would violate U.S. criminal law if committed in the United States.

§2806. Establishment and operations of National Electronic Technologies Center.—This section establishes a National Electronic Technologies Center (''NET Center'') to serve as a focal point for information and assistance to federal, state, and local law enforcement authorities to address the technical difficulties of obtaining plaintext of communications and electronic information through the use of encryption, steganography, compression, multiplexing, and other techniques.

TITLE III—EXPORTS OF ENCRYPTION PRODUCTS

SEC. 301. Commercial Encryption Products.

(a) PROVISIONS APPLICABLE TO COMMERCIAL PRODUCTS.—This title applies to *all* encryption products other than those specifically designed or modified for military use.

(b) CONTROL BY SECRETARY OF COMMERCE.—This section grants exclusive authority to the Secretary of Commerce (the ''Secretary'') to control commercial encryption product exports.

SEC. 302. License Exception for Mass Market Products.

(a) EXPORT CONTROL RELIEF.—The Act permits export under a license exception of generally available, mass market, encryption products, which by their nature are uncontrollable given the volume sold and ease of distribution, without a license or restrictions, other than those permitted under this Act, after a 1-time 15-day technical review by the Secretary.

(b) DEFINITIONS.—This section defines ''generally available'' as a product offered for sale, license, or transfer, including over-the-counter sales, mail or phone order transactions, electronic distribution, or sale on approval and not designed, developed or customized by the manufacturer for specific purchasers (except for installation or configuration parameters).

(c) COMMERCE DEPARTMENT ASSURANCE.—This section permits requests from manufacturers or exporters to the Secretary for written assurance that a product is ''generally available,'' and requires that the Secretary notify the petitioner of a decision within 30 days. This section prohibits imposition of liability or sanctions on petitioners who receive such a written assurance for failing to obtain an export license.

SEC. 303. License Exception for Products Without Encryption Capable of Working With Encryption Products.

This section permits export under a license exception of products, which do not provide any encryption themselves, but that are capable of working with encryption products, without restriction other than those permitted under this Act, after a 1-time, 15 day technical review by the Secretary.

SEC. 304. License Exception For Product Support and Consulting Services.

(a) NO ADDITIONAL EXPORT CONTROLS IMPOSED IF UNDERLYING PRODUCT COVERED BY LICENSE EXCEPTION.—This section permits export of product support and consulting services, including technical assistance and technical data associated with the installation and maintenance of mass market encryption products or products capable of working with encryption products without an export license and without restrictions other than those permitted under this Act.

(b) DEFINITIONS.—This section defines technical assistance as services, such as instruction, skills training, working knowledge, consulting services and transfer of technical data. ''Technical data'' is defined as information, including blueprints, plans, diagrams, models, formulae, table, engineering designs and specifications, manuals and instructions.

SEC. 304. License Exception When Comparable Foreign Products Available.

(a) FOREIGN AVAILABILITY STANDARD.—This section permits unrestricted export of customized encryption hardware and software products (i.e., not generally available mass market products) if a foreign encryption product using the same or greater key length or providing comparable security is, or will within 18 months, be commercially available outside the United States.

(b) DETERMINATION OF FOREIGN AVAILABILITY.—This section establishes an Encryption Export Advisory Board (the ''Board''), which is chaired by the Under Secretary of Commerce for Export Administration, with seven Presidential appointees (3 government and 4 private sector representatives); and four Congressional appointees from the private sector. The Board is required to meet at the call of the Chairman, or if there are any pending applications for a license exception, the Board shall meet at least once every 30 days.

The primary duties of the Board shall be to determine whether comparable foreign encryption products are commercially available outside the United States. The decision is by majority vote, and must be made within 30 days of receipt of application for a license exception. The Board must notify the Secretary of its determination, and submit a report to the President within 30 days. Board meetings are exempt from the Federal Advisory Committee Act.

The Secretary is required to approve or disapprove each Board determination within 30 days of receipt of that determination, notify the Board of the approval or disapproval, and publish notice of the approval or disapproval in the Federal Register. The notice shall include an explanation in detail of the reasons for the decision, including why and how continued export controls will be effective and the amount of lost sales and market share of U.S. encryption product which resulted. Judicial review of the Secretary's decision to disapprove a Board decision that a product is commercially available is permitted.

(c) INCLUSION OF COMPARABLE FOREIGN ENCRYPTION PRODUCTS IN A UNITED STATES PRODUCT NOT BAISS FOR EXPORT CONTROLS.—This section permits export under a license exception of products incorporating or employing a foreign encryption product in the way it was intended to be used and that the Board has determined to be commercially available outside the United States, without an export license and without restrictions other than those under the Act, after a 1-time 15 day review by the Secretary.

SEC. 306. No Export Controls on Encryption Products Used For Nonconfidentiality Purposes.

(a) PROHIBITION ON NEW CONTROLS.—This section prohibits restrictions on encryption exports used for nonconfidentiality purposes such as authentication, integrity, digital signatures, nonrepudiation and copy protection.

(b) NO REINSTATEMENT OF CONTROLS ON PREVIOUSLY DECONTROLLED PRODUCTS.—This section prohibits administratively imposed encryption controls on previously decontrolled products not requiring an export license as of January 1, 1998.

SEC. 307. Applicability of General Export Controls.

(a) SUBJECT TO TERRORISTS AND EMBARGO CONTROLS.—Nothing in the Act shall limit the President's authority under the International Emergency Economic Powers Act, the Trading With the Enemy Act, or the Export Administration Act to prohibit export of encryption products to countries that have repeatedly provided support for international terrorism, or impose an embargo on exports or imports from a specific country.

(b) SUBJECT TO SPECIFIC DENIALS FOR SPECIFIC REASONS.—The Secretary is required to prohibit export of encryption products to an individual or organization in a specific foreign country identified by the Secretary, if the Secretary determines that there is substantial evidence that such encryption product will be used for military or terrorist end-use, including acts against the critical infrastructure of the United States.

(c) OTHER EXPORT CONTROLS REMAIN APPLICABLE.—Encryption products remain subject to all export controls imposed for reasons other than the existence of encryption capabilities, and the Secretary retains the authority to control exports of products for reasons other than encryption.

SEC. 308. Foreign Trade Barriers to United States Products.

The Secretary, in consultation with the United States Trade Representative, is required within 180 days of enactment of the Act to: (1) identify foreign barriers to the export of U.S. encryption products; (2) initiate appropriate actions to address such barriers; and (3) submit to Congress a report on the actions taken under this section.

Mr. BURNS. Mr. President, I stand before the chamber today in support of the e-Privacy Act because the very future of electronic commerce on the Internet is being held hostage to cold-war era export controls. These outdated regulations tie the hands of the U.S. high technology industry and pose a threat to privacy and security of all Americans who use the Internet. Despite some small concessions by the Administration, the competitive advantage of the U.S. high technology industries and the privacy and security of our citizens remain trapped by the Clinton Administration's outdated policy.

The e-Privacy Act will relax current export controls on encryption technologies so that U.S. companies can effectively compete in the global marketplace. The bill will also prevent the government from mandating risky and expensive ''key-recovery'' or ''key-escrow'' encryption systems domestically. It's a good bill, it has broad support from the computer and communications industry, Internet users, and privacy advocates from both the left and right of the political spectrum.

The Clinton Administration has expressed concerns about the impact the e-Privacy Act would have on the legitimate needs of law enforcement and national security. My colleagues and I do not take their concerns lightly. Several provisions in the e-Privacy Act address the Administration's valid concerns while at the same time freeing U.S. companies to effectively compete in the global marketplace, and ensuring that the American people can trust the Internet as a secure means of commerce, education, and free expression of ideas.

The e-Privacy Act would create a National Electronic Technology Center (''NET Center'') to serve as a central point for information and assistance to federal, state, and local law enforcement authorities to address the technical difficulties of obtaining electronic information because of encryption. National security and law enforcement would be given seats at the table in making these determinations. Once again, I am very sensitive to the legitimate needs of national security and law enforcement, and I think the provisions made in the e-Privacy Act address them.

The e-Privacy Act also extends to citizens that same privacy rights that they have in their homes to their digital property in cyberspace. The bill would require a court order or subpoena to obtain either the plaintext or decryption key from their parties. I believe that this is the correct approach.

Citizens are also specifically given the right to use whatever kind of encryption software at whatever strength they choose. The bill recognizes the folly of requiring the government to create procedures to license ''key certificate authorities'' and ''key-recovery agents,'' as well as require the development of a massive and complicated infrastructure to ensure that the government could recover the right key out of the hundreds of millions of keys in real time.

On many occasions, the world's leading cryptographers concluded that building such a key recovery infrastructure would be prohibitively expensive and would create a less secure network. The bill recognizes that mandatory key escrow will never work, no one will use it and certainly no criminals or other bad actors will use a system that is immediately accessible by the government.

I urge my colleagues to support the e-Privacy Act, which I feel is the true compromise package. We all have the same goals in mind—allowing for the

continued growth of high tech industries while not harming national security. If we move forward with the compromise bill being offered today, I am confident we can do both.

By Mr. THOMPSON (for himself and Mr. GLENN):

S. 2068. A bill to clarify the application of the Unfunded Mandates Reform Act of 1995, and for other purposes; to the Committee on the Budget and the Committee on Governmental Affairs, jointly, pursuant to the order of August 4, 1977, with instructions that if one Committee reports, the other committee have 30 days to report or be discharged.

UNFUNDED MANDATES LEGISLATION

Mr. THOMPSON. Mr. President, I rise today to introduce a bill to clarify the application of the Unfunded Mandates Reform Act of 1995. On its face, this legislation is necessary to correct the Congressional Budget Office's interpretation of the law as it applies to large entitlement programs. But more fundamentally, it is a bill to force Congress to abide by the spirit of the law we passed in 1995 to discourage Congress from imposing costly new mandates on States and local governments.

CBO's performance in fulfilling its responsibilities under the Unfunded Mandates Reform Act has been commendable. CBO cost estimates have been timely and sound, and analysts have been responsive. However, I have serious concern that CBO is misinterpreting the definition of ''Federal intergovernmental mandate'' as provided in the law. The result is a loophole that makes the Unfunded Mandates Reform Act inoperative for two-thirds of all federal aid to all governments for all purposes. Every State, every municipality is justifiably concerned; indeed, it is with the strong backing of the National Governors' Association that I introduce this bill today.

The Unfunded Mandates Reform Act defined ''federal intergovernmental mandate'' with the intent to cover new requirements or a cap on the federal share of costs under Medicaid or other large entitlement programs—unless the legislation imposing the new mandates also provides new flexibility in the program to offset the cost. However, CBO has taken the position that existing flexibility is sufficient to offset the cost of new mandates. For example, CBO has determined that the current ability of States to reduce ''optional'' Medicaid services is, in effect, the flexibility called for in the law. If this had been the intent of the drafters, there would have been no reason for them to cover Medicaid under the Act in the first place. CBO's interpretation of the law largely removes the point of order as a tool to discourage new mandates or cost-shifts to States under the large entitlement programs where mandates tend to be the most burdensome and expensive.

Let's stop for a moment and consider why it is so important that we act to correct this problem. Congress passed the Unfunded Mandates Reform Act in 1995 with the recognition that State and local governments are not wayward subordinates who cannot be trusted to run their own affairs, nor are they just more entities for the Federal Government to regulate. They are our partners in government. The Unfunded Mandates Reform Act was intended to force Congress to stop and think twice before violating this partnership. It does not preclude new mandates, but it does give any member the right to raise a point of order against new mandates which would cost States or localities more than fifty million dollars.

To avoid the point of order, the House and Senate intended that the flexibility required under the Act be new flexibility, concomitant with the mandate-imposing legislation, for States to amend their responsibilities to provide ''required services''—not optional services. CBO is not reading the law as Congress intended. The bill I am introducing today amends the Unfunded Mandates Reform Act to clarify that new flexibility is required to offset any new federally-imposed costs that States or localities will incur under large entitlement programs.

I am pleased that Senator GLENN, an original cosponsor and conferee on the Unfunded Mandates Reform Act of 1995, has joined me in cosponsoring this bill to clarify its application.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 2068

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. FEDERAL INTERGOVERNMENTAL MANDATE.

Section 421(5)(B) of the Congressional Budget and Impoundment Control Act of 1974 (2 U.S.C. 658(5)(B)) is amended—

(1) by striking ''the provision'' after ''if'';

(2) in clause (i)(I) by inserting ''the provision'' before ''would'';

(3) in clause (i)(II) by inserting ''the provision'' before ''would''; and

(4) in clause (ii)—

(A) by inserting ''that legislation, statute, or regulation does not provide'' before ''the State''; and

(B) by striking ''lack'' and inserting ''new or expanded''.

By Mr. DEWINE:

S. 2070. A bill to provide for an Underground Railroad Educational and Cultural Program; to the Committee on Labor and Human Resources.

THE UNDERGROUND RAILROAD EDUCATIONAL AND CULTURAL ACT

Mr. DEWINE. Mr. President, today I am introducing the Underground Railroad Educational and Cultural Act. This legislation will provide for the establishment of programs to research, display, interpret, and collect artifacts relating to the history of the Underground Railroad.

Let me tell you how important the Underground Railroad is to Ohio—and to me personally. In the 20 years prior to the Civil War, more than 40,000 slaves escaped bondage and made their way to free soil on the trails of the Underground Railroad. More than 150 key Underground Railroad sites have been identified in Ohio—sites that symbolized freedom for thousands of enslaved Americans.

When I visit these places, it gives me some real cause for hope about the future of America. When we talk about race relations in this country, we would do well to remind ourselves that at one of the darkest times in our nation's history—the period of slavery—some blacks and whites took immense personal risks to work together to liberate slaves.

That is the part of the American story that we should be proud of—and build on. In Ohio, we are very proud of the part our ancestors played in this great story—and why I think this legislation is so important.

Mr. President, I ask my colleagues to support this legislation. It is very important to recognize this period in our history.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 2070

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. UNDERGROUND RAILROAD EDUCATIONAL AND CULTURAL PROGRAM.

(a) SHORT TITLE.—This section may be cited as the ''Underground Railroad Educational and Cultural Act''.

(b) PROGRAM ESTABLISHED.—The Secretary of Education, in consultation and cooperation with the Secretary of the Interior, is authorized to make grants to 1 or more nonprofit educational organizations that are established to research, display, interpret, and collect artifacts relating to the history of the Underground Railroad.

(c) GRANT AGREEMENT.—Each nonprofit educational organization awarded a grant under this section shall enter into an agreement with the Secretary of Education. Each such agreement shall require the organization—

(1) to establish a facility to house, display, and interpret the artifacts related to the history of the Underground Railroad;

(2) to demonstrate substantial private support for the facility through the implementation of a public-private partnership between a State or local public entity and a private entity for the support of the facility, which private entity shall provide matching funds for the support of the facility in an amount equal to 4 times the amount of the contribution of the State or local public entity, except that not more than 20 percent of the matching funds may be provided by the Federal Government;

(3) to create an endowment to fund any and all shortfalls in the costs of the on-going operations of the facility;

(4) to establish a network of satellite centers throughout the United States to help disseminate information regarding the Underground Railroad throughout the United States, if such satellite centers raise 80 percent of the funds required to establish the

satellite centers from non-Federal public and private sources;

(5) to establish the capability to electronically link the facility with other local and regional facilities that have collections and programs which interpret the history of the Underground Railroad; and

(6) to submit, for each fiscal year for which the organization receives funding under this section, a report to the Secretary of Education that contains—

(A) a description of the programs and activities supported by the funding;

(B) the audited financial statement of the organization for the preceding fiscal year;

(C) a plan for the programs and activities to be supported by the funding as the Secretary may require; and

(D) an evaluation of the programs and activities supported by the funding as the Secretary may require.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $6,000,000 for fiscal year 1999, $6,000,000 for fiscal year 2000, $6,000,000 for fiscal year 2001, $3,000,000 for fiscal year 2002, and $3,000,000 for fiscal year 2003.

ADDITIONAL COSPONSORS

S. 249

At the request of Mr. D'AMATO, the name of the Senator from California (Mrs. BOXER) was added as a cosponsor of S. 249, a bill to require that health plans provide coverage for a minimum hospital stay for mastectomies and lymph node dissection for the treatment of breast cancer, coverage for reconstructive surgery following mastectomies, and coverage for secondary consultations.

S. 632

At the request of Mr. KOHL, the name of the Senator from Oregon (Mr. SMITH) was added as a cosponsor of S. 632, a bill to amend the Internal Revenue Code of 1986 with respect to the eligibility of veterans for mortgage revenue bond financing, and for other purposes.

S. 719

At the request of Mr. WELLSTONE, the name of the Senator from Wisconsin (Mr. FEINGOLD) was added as a cosponsor of S. 719, a bill to expedite the naturalization of aliens who served with special guerrilla units in Laos.

S. 852

At the request of Mr. LOTT, the name of the Senator from Wyoming (Mr. ENZI) was added as a cosponsor of S. 852, a bill to establish nationally uniform requirements regarding the titling and registration of salvage, nonrepairable, and rebuilt vehicles.

S. 1089

At the request of Mr. SPECTER, the name of the Senator from North Dakota (Mr. DORGAN) was added as a cosponsor of S. 1089, a bill to terminate the effectiveness of certain amendments to the foreign repair station rules of the Federal Aviation Administration, and for other purposes.

S. 1220

At the request of Mr. DODD, the name of the Senator from Massachusetts (Mr. KENNEDY) was added as a cosponsor of S. 1220, a bill to provide a process for declassifying on an expedited basis certain documents relating to human rights abuses in Guatemala and Honduras.

S. 1244

At the request of Mr. GRASSLEY, the name of the Senator from Missouri (Mr. ASHCROFT) was added as a cosponsor of S. 1244, a bill to amend title 11, United States Code, to protect certain charitable contributions, and for other purposes.

S. 1251

At the request of Mr. D'AMATO, the name of the Senator from Iowa (Mr. HARKIN) was added as a cosponsor of S. 1251, a bill to amend the Internal Revenue Code of 1986 to increase the amount of private activity bonds which may be issued in each State, and to index such amount for inflation.

S. 1252

At the request of Mr. D'AMATO, the names of the Senator from Iowa (Mr. HARKIN) and the Senator from Missouri (Mr. BOND) were added as cosponsors of S. 1252, a bill to amend the Internal Revenue Code of 1986 to increase the amount of low-income housing credits which may be allocated in each State, and to index such amount for inflation.

S. 1321

At the request of Ms. MIKULSKI, her name was added as a cosponsor of S. 1321, a bill to amend the Federal Water Pollution Control Act to permit grants for the national estuary program to be used for the development and implementation of a comprehensive conservation and management plan, to reauthorize appropriations to carry out the program, and for other purposes.

S. 1344

At the request of Mr. BROWNBACK, the name of the Senator from Arizona (Mr. KYL) was added as a cosponsor of S. 1344, a bill to amend the Foreign Assistance Act of 1961 to target assistance to support the economic and political independence of the countries of South Caucasus and Central Asia.

S. 1464

At the request of Mr. HATCH, the name of the Senator from Connecticut (Mr. DODD) was added as a cosponsor of S. 1464, a bill to amend the Internal Revenue Code of 1986 to permanently extend the research credit, and for other purposes.

S. 1529

At the request of Mr. BIDEN, his name was added as a cosponsor of S. 1529, a bill to enhance Federal enforcement of hate crimes, and for other purposes.

S. 1609

At the request of Mr. FRIST, the name of the Senator from Vermont (Mr. JEFFORDS) was added as a cosponsor of S. 1609, a bill to amend the High-Performance Computing Act of 1991 to authorize appropriations for fiscal years 1999 and 2000 for the Next Generation Internet program, to require the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet to monitor and give advice concerning the development and implementation of the Next Generation Internet program and report to the President and the Congress in its activities, and for other purposes.

S. 1645

At the request of Mr. ABRAHAM, the name of the Senator from Minnesota (Mr. GRAMS) was added as a cosponsor of S. 1645, a bill to amend title 18, United States Code, to prohibit taking minors across State lines to avoid laws requiring the involvement of parents in abortion decisions.

S. 1723

At the request of Mr. ABRAHAM, the names of the Senator from Missouri (Mr. BOND), the Senator from North Carolina (Mr. FAIRCLOTH), the Senator from Idaho (Mr. CRAIG), and the Senator from Washington (Mr. GORTON) were added as cosponsors of S. 1723, a bill to amend the Immigration and Nationality Act to assist the United States to remain competitive by increasing the access of the United States firms and institutions of higher education to skilled personnel and by expanding educational and training opportunities for American students and workers.

S. 1981

At the request of Mr. HUTCHINSON, the name of the Senator from Kansas (Mr. BROWNBACK) was added as a cosponsor of S. 1981, a bill to preserve the balance of rights between employers, employees, and labor organizations which is fundamental to our system of collective bargaining while preserving the rights of workers to organize, or otherwise engage in concerted activities protected under the National Labor Relations Act.

S. 2017

At the request of Mr. D'AMATO, the names of the Senator from Iowa (Mr. HARKIN), and the Senator from Kentucky (Mr. FORD) were added as cosponsors of S. 2017, a bill to amend title XIX of the Social Security Act to provide medical assistance for breast and cervical cancer-related treatment services to certain women screened and found to have breast or cervical cancer under a Federally funded screening program.

S. 2053

At the request of Mr. WARNER, the name of the Senator from Virginia (Mr. ROBB) was added as a cosponsor of S. 2053, a bill to require the Secretary of the Treasury to redesign the $1 bill so as to incorporate the preamble to the Constitution of the United States, the Bill of Rights, and a list of Articles of the Constitution on the reverse side of such currency.

SENATE CONCURRENT RESOLUTION 88

At the request of Mr. D'AMATO, the names of the Senator from North Dakota (Mr. CONRAD) and the Senator from Nevada (Mr. REID) were added as cosponsors of Senate Concurrent Resolution 88, A concurrent resolution calling on Japan to establish and maintain an open, competitive market for consumer photographic film and paper and