CONGRESSIONAL BUDGET OFFICE
MANDATES STATEMENT

September 19, 1997

H.R. 695
Security and Freedom through Encryption ('SAFE') Act of 1997

As reported by the House Permanent Select Committee on Intelligence
on September 16, 1997

SUMMARY

H.R. 695 would establish controls on domestic encryption technology. Specifically, the bill would require public network service providers that offer encryption services, and manufacturers, distributors, and importers of encryption products to include features or functions that permit duly authorized individuals to gain immediate access to the encrypted material without the knowledge or cooperation of the user of that material. Thus, it would impose a federal mandate on a wide variety of entities—private and public—selling goods and services for electronic communication, including many producers and sellers of computer hardware and software. CBO estimates that the total direct costs of complying with this mandate could be between $0.2 billion and $2.0 billion per year. Most of those costs would fall on private firms or individuals and thus would exceed the statutory threshold ($100 million in 1996, adjusted annually for inflation) for private-sector mandates established in the Unfunded Mandates Reform Act (UMRA). It is less clear whether the costs imposed on state and local governments would exceed the threshold established for intergovernmental mandates ($50 million in 1996, adjusted annually for inflation).

This statement represents CBO's estimate of the costs of mandates contained in H.R. 695, excluding provisions that are included under Title III, Exports of Encryption. Those provisions are excluded from consideration under Section 4 of UMRA because they are considered necessary for national security purposes. CBO provided an estimate of federal cost for H.R. 695 on September 16, 1997.

MANDATES CONTAINED IN BILL

Section 2803 would prohibit the sale of any encryption product that did not include features permitting "immediate access to plaintext or immediate decryption capabilities." Section 2804 would require that public network service providers and manufacturers, distributors, and importers that offer encryption products or services provide capabilities that allow immediate access to a readable format of the encrypted information without the knowledge of the user. A court order or warrant would be required to gain access to decryption capabilities.

The bill does not specify the means, mechanism, or technological method required to provide the readable information. The bill would require that the Attorney General publish technical requirements and functional criteria for complying with the requirements of the bill. The Attorney General also would issue advisory opinions as to whether the network service providers and manufacturers, distributors and importers of encryption products meet those requirements.

This bill would affect encrypted services and products intended for sale in the United States after January 31, 2000. A grandfather provision would exclude encryption products purchased or in use prior to that date.

The definitions of "encryption" and "encryption product" contained in Section 101 (8) and (9) are sufficiently broad as to potentially encompass most digital technology because it transforms data or communications into an unreadable format. Thus, entities that could be directly affected by the requirements of H.R. 695 include Internet service providers, producers of computer hardware and software, telecommunications firms, and cable television providers. Some of these entities are state and local governments, including universities.

CBO assumes that the regulations promulgated by the Attorney General would limit the scope of activity covered, since most telecommunications, television, and general-use computer software products are already easily decoded or "decrypted." For example, cable television providers typically offer premium services, such as HBO, in an encrypted form, which must be decoded by a cable box attached to the receiver. Although a cable television provider could be subject to the requirements of H.R. 695, it would not incur any costs to comply with the mandate to provide decryption capability because that capability already exists. Similarly, providers of digital telecommunications and producers of most standard computer hardware and software could easily comply with the bill.

ESTIMATED DIRECT COST TO THE PRIVATE SECTOR

CBO's estimate of the costs of complying with the requirements of H.R. 695 encompasses a very broad range—between $200 million and $2.0 billion per year. This range is consistent with the wide variety of opinions held by encryption experts that were consulted by CBO. Those experts differ widely on how they interpret the legal requirements of the bill and on how individual firms might meet those requirements, or even whether it is technologically feasible to do so. Much depends on

the technical requirements and functional criteria for complying with decryption that would be established by the Attorney General, under Section 2803(c). Firms that provide general users access to the Internet, electronic mail, and similar services (such as so called "virtual private networks") are among those likely to experience the most difficulty in developing systems that meet the requirements of H.R. 695. CBO was unable to obtain any information from the Department of Justice that would help narrow the range of this estimate.

Encryption products are still being defined by the market and are currently in flux. By requiring immediate access to decrypted information without the knowledge of the user, this bill would have a substantial effect on the cost of developing encryption products, the types of products and services offered for sale, and the demand for those products. CBO's estimate is based on a detailed examination of the core costs of operating key recovery systems—that is, a system that allows access to a copy of the key needed to decrypt encrypted information—and a more speculative survey of other potential costs. Other costs could include initial capital costs, research and product development costs, the sales that the mandated entities might lose because of reduced functionality of their product or service, and costs associated with ensuring access to hard disks, databases, or other forms of electronically stored information that are not transmitted over communications systems.

CBO cannot readily determine how the participants in such a nascent market would react to the requirements of H.R. 695. Specifically, we are unable to determine which products and services would be directly affected or which technological responses by suppliers would prove most feasible, cost-effective, and acceptable to the Attorney General. Neither are we able to predict how users would react to the newly imposed requirements. At this juncture, it seems likely that both producers and consumers will adopt a variety of solutions, depending upon their individual circumstances. Some producers and suppliers of affected products and services may easily meet the new requirements at little or no cost; others would find it costly, and perhaps even technologically impossible. Users could respond to the mandate by limiting the overall demand for encryption products, either because they would be inherently less useful, or because they would become too expensive.

Background

Encryption is the transformation or scrambling of data or communications to an unreadable format by using a mathematical algorithm or formula, for the purpose of protecting the content of such data or communications. Encryption technology is used to protect data and communications, such as trade secrets, medical records, data used in the operation of critical information systems (for example the air traffic control system and financial transaction networks), the signals of premium cable channels, and electronic mail. An encryption product can be either hardware- or software-based. Typically, an electronic key is used to decrypt or unscramble the data or communication into a readable format.

Revenues generated by the sales of U.S. encryption products and services (including hardware and software) were between $500 million and $1 billion in 1996 and are growing rapidly. The Commerce Department describes the growth of this market as "explosive," especially with the advent of commerce on the Internet. Encryption software that would facilitate credit card and other secure transactions over the Internet is widely perceived to be a requirement for the development of electronic commerce. The increased use of e-mail is also spurring the demand for inexpensive, easy-to-use encryption to ensure confidentiality comparable to that of conventional mail.

Approximately 3,500 companies offer access to the Internet in the U.S., providing service to about 40 million accounts. Revenues of Internet service providers are in the range of $3 billion to $4 billion annually. The number of accounts has risen dramatically in the last few years and is forecast to continue to do so. Few Internet service providers offer encryption services directly. However, they typically offer both e-mail software and Internet browsers that have encryption capabilities. CBO estimates that approximately 100 million computers will be connected to public communications networks in 2000.

Basis of Estimate

CBO's estimate of the costs of complying with the requirements of H.R. 695 is based on establishing a feasible range of costs, given substantial uncertainties and limited information. Thus, both the bottom ($0.2 billion) and top ($2.0 billion) end of the estimated range are based on fairly extreme assumptions. Those endpoints should be viewed, respectively, as the lowest and highest possible costs (although, even at those endpoints some uncertainty still exists). The costs most likely lie between those two figures.

CBO's estimates of costs are based on two components—operating costs and all other costs. According to the cryptology literature and experts consulted by CBO, the major expense of complying with this mandate would be the costs associated with operating and maintaining a key recovery system. Thus, CBO has focused on quantifying those core costs, which range in our estimates between $100 million and $1.6 billion annually. The size of that range derives, in part, because no one has ever implemented a key recovery system as broad as that contemplated in this legislation. The second component of costs, encompasses all other types of costs—such as initial capital costs, research and product development costs, lost net revenues from reduced sales, and costs associated with those who cannot use the lowest-cost technology. Those cost are estimated to add $100 million to the low end of the range and $400 million to the high end.

An important assumption relates to the requirement for "immediate decryption or access to plaintext" of any encrypted document, without the knowledge of the user of the document. That requirement could be met in a variety of ways. For the low-end estimate, CBO relied on information about the cost of currently available commercial technology, which would add about $1 a year to the cost of using a computer. That operational cost, when multiplied by the 100 million computers that CBO

estimates would be connected to communications systems in 2000, yields an estimate of $100 million annually.

Adding other costs raises the low-end estimate of total costs to about $200 million. One component of other costs arises because it is doubtful that the lowest-cost solution will fit either the needs of all users or the requirements of the Attorney General. In the opinion of most experts, some firms—notably, Internet service providers and large organizations that maintain networks connected to the Internet—would most likely need to establish costly key recovery centers. In part, the need for such a secure center derives from the likelihood that encryption software would need to be designed to allow undetected access for decryption. The encrypted document would be able to be opened by a key, which would be retained by the center. Safeguarding the keys would become a security concern, and the center itself would be a valuable target for criminals. Operating a secure center for holding and protecting decryption keys could cost between $0.5 million and $1.0 million per year, based on a need to be staffed around the clock. That estimate does not include the initial cost of equipping and housing such a center. Centers may be operated by third parties, under contract, or by very large users, such as major corporations or Internet service providers, but the costs would be about the same regardless of who operated them.

The high end of CBO's estimate of operating costs derives from testimony by the National Security Agency; that estimate was for a cost of about $16 per computer. Multiplying by 100 million computers yields an estimate of $1.6 billion, and adding other costs raises the total estimate to $2.0 billion.

Another method of obtaining estimates similar to those described above is based on a more detailed examination of one of the components of "other costs," namely lost revenues from reduced sales of encryption-capable products and services. In the estimates described above, lost sales are assumed to be relatively small, ranging in value between less than $100 million and $400 million. However, the upper end of the range is limited only by the size of the overall market for encryption products and services. That market is estimated by CBO to be roughly $2.0 billion in 2000. Although CBO does not believe that the entire encryption market would be eliminated, H.R. 695 could have a substantial impact on the development of that market and its ultimate size.

Two scenarios examined by CBO indicate that private-sector mandate costs are most likely to be at an intermediate level between the extreme high and low, based on the effect that mandated requirements could have on the market. One scenario is that producers and providers of encryption products and services would cut back significantly on their willingness to offer such products or services, because they would be unwilling to bear the costs or legal liabilities that would be associated with meeting the bill's requirements. For example, products that embody cryptography features—such as Internet browsers and database, spreadsheet, and word processor programs—may drop such features so as to avoid the costs and liability inherent in key recovery systems. Another scenario is that the added costs and changed functionality of products and services would deter some potential users and limit the size of the market. For example, if the costs are sufficiently high, fewer

persons would choose to provide their credit card over the Internet. Instead, most would use the current method of relying on a toll-free phone service for their purchases.

CBO concludes that Internet service providers and others who are basing their business strategies on the expectation of substantial growth in markets dependent on encryption, such as electronic commerce, may find their opportunities limited, but they may very well be able to maintain their current customer base by offering services that exclude or modify encryption capabilities.

ESTIMATED COSTS TO STATE, LOCAL, AND TRIBAL GOVERNMENTS

H.R. 695 contains an intergovernmental mandate as defined in UMRA, because state and local governments that offer Internet access and other computer services to the public would meet the bill's definition of "network service provider." As such, they would be required by January 31, 2000, to ensure that any encryption products or services they provide enable the immediate decryption or access to the plaintext of encrypted data. Because of uncertainty about how many state and local governments would be affected and about the alternatives that would be available to them, CBO cannot estimate whether the cost of complying with this mandate would exceed the threshold established in UMRA. However, if total compliance costs are closer to the high end of the range specified above ($2 billion), state and local governments would only have to bear about 3 percent of those costs in order for the threshold to be exceeded.

A number of states and localities (including public colleges and universities) currently offer Internet access to the public. For example, localities in Maryland are cooperating with the state's SAILOR program to provide public access to on-line government resources and to the Internet. Citizens can utilize SAILOR by visiting computer terminals placed in libraries and shopping malls or by dialing into the network with their own computer and modem. Some Maryland localities are also offering Internet accounts for sale.

As described above, few Internet service providers offer encryption services directly. However, like private providers, states and localities offering Internet access typically provide e-mail and browser software with encryption capabilities. In addition to Internet access, public colleges and universities offer the public other computer services and products that might be affected by the bill. CBO is unaware of any data that indicate how many governments across the country are providing Internet or other computer services to the public. Furthermore, given how quickly the Internet is evolving, CBO cannot predict how many state and local governments will be offering computer-related services to the public by 2000, when the mandate would become effective.

To comply with the mandate in the bill, states and localities that are network service providers could purchase software that meets the bill's requirements. This software would likely be more expensive than what they otherwise would have purchased. For reasons described above, however, it is uncertain how much more expensive it would be. Alternatively, states and localities could choose software lacking any encryption capabilities or software grandfathered by the bill. This choice

would allow state and local governments to avoid higher costs, but it would limit the usefulness of the computer services they provide.

Although state and local governments would have to comply with the bill's requirements, they would also benefit from the ability to gain access to encrypted data. State and local law enforcement agencies would be able to obtain court orders granting access to the plaintext of encrypted data or to decryption information. The bill would not enlarge or modify the circumstances under which government entities are entitled to intercept or obtain information.

PREVIOUS CBO ESTIMATES:

CBO provided cost estimates for H.R. 695 as ordered reported by the House Committee on the Judiciary on May 14, 1997, as ordered reported by the House Committee on International Relations on July 22, 1997, and as ordered reported by the House Committee on National Security on September 9, 1997. Those bills did not contain any new private-sector mandates, but all three contained the same intergovernmental mandate on state governments. They would have prohibited states from requiring people to make encryption keys available to another person or entity. CBO estimated that states would bear no costs as a result of that mandate because none currently require the registration or availability of such keys.

ESTIMATE PREPARED BY:

Private-Sector Mandates—Philip Webre and Jean Wooster
Intergovernmental Mandates—Pepper Santalucia

ESTIMATE APPROVED BY:

Jan Paul Acton
Assistant Director for
Natural Resources and Commerce

Paul N. Van de Water
Assistant Director for
Budget Analysis