

to the substances that are subject to trade control with non-Parties; and the addition of a licensing requirement for import and export of controlled substances. The 1997 Amendment will constitute a major step forward in protecting public health and the environment from potential adverse effects of stratospheric ozone depletion.

By its terms, the 1997 Amendment was to have entered into force on January 1, 1999, provided that at least 20 states had deposited their instruments of ratification, acceptance, or ap-

proval. However, because this condition was not met until August 12, 1999, the 1997 Amendment will enter into force on November 10, 1999.

I recommend that the Senate give early and favorable consideration to the 1997 Amendment to the Montreal Protocol and give its advice and consent to ratification.

WILLIAM J. CLINTON

The White House,  
September 16, 1999.

## Message to the Congress Transmitting Proposed Legislation on Security of Electronic Information

*September 16, 1999*

*To the Congress of the United States:*

I am pleased to transmit for your early consideration and speedy enactment a legislative proposal entitled the "Cyberspace Electronic Security Act of 1999" (CESA). Also transmitted herewith is a section-by-section analysis.

There is little question that continuing advances in technology are changing forever the way in which people live, the way they communicate with each other, and the manner in which they work and conduct commerce. In just a few years, the Internet has shown the world a glimpse of what is attainable in the information age. As a result, the demand for more and better access to information and electronic commerce continues to grow—among not just individuals and consumers, but also among financial, medical, and educational institutions, manufacturers and merchants, and State and local governments. This increased reliance on information and communications raises important privacy issues because Americans want assurance that their sensitive personal and business information is protected from unauthorized access as it resides on and traverses national and international communications networks. For Americans to trust this new electronic environment, and for the promise of electronic commerce and the global information infrastructure to be fully realized, information systems must provide methods to protect the data and communications of legitimate users. Encryption can address this need because encryption can be used to protect

the confidentiality of both stored data and communications. Therefore, my Administration continues to support the development, adoption, and use of robust encryption by legitimate users.

At the same time, however, the same encryption products that help facilitate confidential communications between law-abiding citizens also pose a significant and undeniable public safety risk when used to facilitate and mask illegal and criminal activity. Although cryptography has many legitimate and important uses, it is also increasingly used as a means to promote criminal activity, such as drug trafficking, terrorism, white collar crime, and the distribution of child pornography.

The advent and eventual widespread use of encryption poses significant and heretofore unseen challenges to law enforcement and public safety. Under existing statutory and constitutional law, law enforcement is provided with different means to collect evidence of illegal activity in such forms as communications or stored data on computers. These means are rendered wholly insufficient when encryption is utilized to scramble the information in such a manner that law enforcement, acting pursuant to lawful authority, cannot decipher the evidence in a timely manner, if at all. In the context of law enforcement operations, time is of the essence and may mean the difference between success and catastrophic failure.

A sound and effective public policy must support the development and use of encryption for

legitimate purposes but allow access to plaintext by law enforcement when encryption is utilized by criminals. This requires an approach that properly balances critical privacy interest with the need to preserve public safety. As is explained more fully in the sectional analysis that accompanies this proposed legislation, the CESA provides such a balance by simultaneously creating significant new privacy protections for lawful users of encryption, while assisting law enforcement's efforts to preserve existing and constitutionally supported means of responding to criminal activity.

The CESA establishes limitations on government use and disclosure of decryption keys obtained by court process and provides special protections for decryption keys stored with third party "recovery agents." CESA authorizes a re-

covery agent to disclose stored recovery information to the government, or to use stored recovery information on behalf of the government, in a narrow range of circumstances (*e.g.*, pursuant to a search warrant or in accordance with a court order under the Act). In addition, CESA would authorize appropriations for the Technical Support Center in the Federal Bureau of Investigation, which will serve as a centralized technical resource for Federal, State, and local law enforcement in responding to the increasing use of encryption by criminals.

I look forward to working with the Congress on this important national issue.

WILLIAM J. CLINTON

The White House,  
September 16, 1999.

## Statement on the Terrorist Attacks in Russia

*September 17, 1999*

On behalf of the American people, I want to extend our deepest condolences to the families of victims of recent bombings in Russia. Our thoughts and prayers are with the loved ones of the nearly 300 people whose lives were tragically lost.

The American people share the world's outrage over these cowardly acts. These attacks were aimed not just at innocent people across Russia; they also targeted fundamental human rights and democratic values, which are cherished by Russia and other members of the international community. We must not allow terrorists to achieve their underlying objective, which is to undermine democratic institutions and individual freedoms.

People across Russia who have been affected by these attacks are now beginning the hard task of rebuilding their lives. Their courage and resilience sets an example for all of us. President Yeltsin and Prime Minister Putin have also made important appeals to their countrymen that these attacks should not lead to new incidents of intolerance or bigotry and that the public should remain calm and unified in response.

In the days and weeks ahead, we will intensify our cooperation with Russian authorities to help prevent terrorist acts. The struggle against terrorism is a long and difficult road, but we must not lose our resolve. America stands ready to work with Russia to protect our citizens from this common threat.

## Statement on the Common Ground Partnerships Initiative

*September 17, 1999*

Today, as we celebrate Citizenship Day and Constitution Week, thousands of individuals in naturalization ceremonies across America are pledging their allegiance to the United States and to the ideals that undergird our Nation.

Like generations of immigrants past, they are driven by a dream, and to achieve that dream, they seek to learn the ways of this land. I believe we can help these new citizens become full participants in American society. That is why