Comments of the United States Government on the European Commission Communication on Combating Computer Crime

The United States welcomes the opportunity to comment on the European Commission's Communication on "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer Related Crime." We congratulate the Commission on its comprehensive treatment of the very complex issues associated with global network security.

As the Commission recognizes, the Internet revolution is rapidly transforming the way we communicate, engage in commerce, and expand people's educational opportunities. As the Internet' s potential to provide unparalleled benefits to society continues to expand, however, we must recognize that global networks also serve as a powerful new medium for those who wish to commit criminal and terrorist acts. Therefore, to truly harness the potential power of the Internet, we must work to foster confidence in the security of our computer networks, and, more importantly, protect our citizens from the very serious threats to public health and safety that cyber crimes pose (see the cyber crime statistics, below).

The real and immediate dangers posed by computer crime require a coordinated international response. The United States and the Commission clearly agree on many of the key principles upon which such coordination must necessarily rest. However, we believe that additional discussion is needed before we can reach broad international consensus on other core issues, such as, for example, thresholds required for criminal liability for expressions of views on the Internet. In an effort to pinpoint some of those areas where additional dialogue would be beneficial, the United States respectfully submits the following comments, which correspond to the basic principles identified by the European Commission in section 7 of the Communication, and the specific legislative and non-legislative proposals addressed in sections 7.1 and 7.2. The United States hopes to have the opportunity to supplement these comments on further consideration of the Communication and the presentations at the March 7, 2001, hearing.

7. Conclusions and Proposals

The United States agrees in general with the key principles outlined in section 7 of the Communication, which must inform a strategy to combat cyber crime. In order for a coordinated international response between government and the private sector to take place, the United States suggests that the European Commission consider using the following points as guiding principles in developing its proposals:

1. Government must protect public safety by investigating network and other computer crimes and ensuring that it has the technical and legal tools to obtain necessary electronic evidence.

2. When private or governmental networks are the victims of crime, government retains its critical role of vindicating society's interests by investigating and prosecuting when appropriate.

3. The private sector should take the lead in protecting private computer networks through vigilant security efforts and cooperation with government. Not only does industry design, build, and operate the infrastructure, systems and related technologies that connect us, it has the know-how and resources to address its security needs.

4. Government must take steps to protect its own computer systems.

5. Government and industry must share information with each other about vulnerabilities so that both can protect systems from attack. We must also share information when an attack occurs and cooperate as necessary to effectively investigate these cases. In this regard, governments must be sensitive to concerns about confidentiality and should avoid imposing undue burdens on private organizations during investigations.

6. Innocent third parties should not be subject to criminal liability for the actions of others, nor should they be liable for legitimate compliance with lawful requests of law enforcement authorities.

7. Governments should avoid imposing unnecessary regulations or restrictions on the Internet. It is important that all stakeholders, including those in the private sector, have meaningful participation in the resolution of issues related to cyber security.

8. Any regulation of conduct involving the use of the Internet requires a careful consideration of different societal interests. Triumph over network crime cannot and must not come at the price of lost privacy and individual freedom. Our domestic investigative tools are subject to strict constitutional, statutory, court-ordered, and internal policy limitations, and we are committed to ensuring that such tools continue to be developed and used consistent with our laws and our much-cherished notions of individual liberty.

9. Government and industry must also work together to educate and raise awareness of computer responsibility and provide resources to empower concerned citizens. In this regard, the US Department of Justice and the Internet Alliance and the Information Technology Association of America ("ITAA") established the Cybercitizen Awareness Program in 1999 to educate children, young adults, and others on the basics of critical information protection and on the limits of acceptable online behavior.

10. The United States government supports cooperation between government, businesses, and universities to discuss joint training programs and resource needs.
11.

12. Because cyber criminals are not confined by national borders or geography, numerous US agencies participate in an initiative coordinated by the State Department to conduct international outreach on critical infrastructure protection. This initiative recognizes that exploitation of information technology is an increasing feature of transnational crime, and that governments around the world must work together to harmonize their substantive and procedural computer crime laws and establish new mechanisms that allow for prompt assistance in investigating and prosecuting computer-related crimes.

13. Governments must also regularly meet with each other to share experience, information, and develop a coordinated operational and policy response, and, where appropriate, remove obstacles that would prevent information sharing. Both the European Union and the United States view the protection of privacy rights as important; governments also have a duty to protect public safety (including prosecuting violations of privacy rights). Data protection procedures in the sharing of law enforcement information must be formulated in ways that do not undercut international cooperation in fighting cyber crime. Recent experience suggests that certain data protection procedures that may work well with respect to the commercial use of data do not translate well to the realities of law enforcement.

14. Components within governments must collaborate among themselves to enact policies that strike the proper balance between protecting the public's safety, the privacy interests of our citizens, and the growth of the Internet as a tool for open communication and legitimate commerce. A comprehensive response is best achieved through direct collaboration between those charged with advancing the growth and security of e-commerce and those charged with protecting the safety of the public.

7.1 Legislative Proposals

- Approximate laws in the area of child pornography and trafficking in persons

With respect to the proposed Council Framework Decisions on combating trafficking in human beings and on combating the sexual exploitation of children and child pornography, the United States believes that revision is required to article 7, paragraph 3 of the trafficking decision, and article 8, paragraph 3 of the pornography decision, which state, in pertinent part:

> "A member State, which, under its laws, does not extradite its own nationals shall take the necessary measures to establish its jurisdiction over and to prosecute, where appropriate, an offence referred to in Articles . . . when it is committed by its own nationals outside its territory."

The current text suggests that a person should be domestically prosecuted without regard to the wishes of a State that has sought extradition. On the other hand, the phrase "where

appropriate" suggests that the requested State has discretion to take no action even if the sole basis for denial of extradition is the nationality of the fugitive.

We initially believe that it is appropriate to highlight, consistent with the EU extradition treaty, that extradition is to be the preferred procedure. Moreover, the article should be more closely aligned with the text of articles 15(3) and 16(10) of the UN Convention on Transnational Organized Crime, which is incorporated by reference into the UN Trafficking in Persons Protocol. Those provisions, which require the views of the requesting State to be taken into account and which require the prosecuting State to act diligently, are the minimum obligation in this area. Furthermore, such provisions would be in keeping with the " aut dedere aut judicare" principles endorsed by the G-8 members last year. The revised text could appear as follows:

> "Each member State should consider permitting extradition of its nationals for the offences referred to in Articles . . .. A member State, which, under its laws, does not extradite its own nationals shall take the necessary measures to establish its jurisdiction over an offence referred to in Articles . . . when it is committed by its own nationals outside its territory. Where the member State has denied extradition on the ground of the nationality of the alleged offender, it shall, at the request of the State seeking extradition, take the necessary measures to submit the case for the purpose of prosecution, and shall take its decision and conduct its proceedings in the same manner as in the case of any other offence of a grave nature under its laws."

- Approximate laws in the area of high-tech crime

We support the Commission's efforts to achieve greater harmonization of the laws that criminalize conduct affecting the confidentiality, integrity, and availability of computer systems and data. With the globalization of communications networks, public safety is increasingly dependent on effective law enforcement cooperation with foreign governments. That cooperation may not be possible, however, if a country does not have the substantive laws in place to prosecute or extradite a perpetrator. In addition, because a number of countries require dual criminality even to render investigative assistance, inadequate laws in just one country that a communication traverses may bring an investigation to a halt.

The dual criminality requirement presents particular problems in high-tech cases because of the speed with which these investigations must proceed and the number of countries that might be involved. It is likely that, in many multinational investigations, perishable data will disappear before a country can ascertain whether the elements of dual criminality are satisfied. In this respect, the draft Council of Europe Convention takes an important first step by requiring countries to respond to foreign evidence-preservation requests without first ascertaining whether dual criminality exists (except in limited cases). Because preservation is typically sought at the initial stages of an investigation to avoid the destruction of perishable evidence, when a preservation request is made, it is often too early in an investigation to determine whether dual criminality will ultimately exist. Thus, in many cases, a dual criminality determination will defeat the very purpose of a preservation request.

Inadequate procedural tools in just one country can also shield criminals from international investigative efforts. Because sophisticated criminals can transmit a communication through multiple carriers and countries before it reaches its intended victim, governments must ensure that those charged with protecting public safety have the tools necessary to keep pace with the technological developments employed by criminals. To identify a criminal in cyber space, investigators must have the technical ability and authority to trace a communication in real-time and must be able to rely on historical transaction records to determine the source of a communication. Moreover, investigators need to rely on communications providers to preserve and access log files, electronic mail, and other records and to do so quickly, before such information is altered or deleted. Currently, however, there are a number of legal impediments in place that prevent law enforcement from obtaining critical evidence.

First, the United States has viewed with some concern the European Commission's recent proposal to extend provisions of the 1997 Data Protection Directive to traffic data over computer networks. A general requirement, with limited exceptions, to erase or anonymize data upon completion of a transaction (as set out in Article 6 of the July 2000 proposed update of the Data Protection directive) will undermine Member States' scope to act in the areas of public security and criminal law although both areas are outside the ambit of the Directive. Access to historic computer traffic data, such as connection logs, in conformity with accepted due process protections, is particularly critical for investigators to identify criminals who commit offenses on networks. Moreover, transactional logs also are an invaluable tool for the private sector to monitor the integrity of its computer systems and protect them from misuse and to learn about system exploits. Service providers could lose their ability to use critical network security methods because they would be obliged to destroy traffic data and logs. We do not believe that permitting public safety and law enforcement exemptions is sufficient; such exemptions, if unimplemented or inconsistently implemented, will lead to inadequate investigative means in some countries, a fragmented approach, and will in effect shield cyber criminals from multijurisdictional criminal investigations. Thus we ask the Commission to ensure that public safety issues are addressed at the EU level by implementing a strong and harmonized approach among Member States so that critical evidence is not destroyed in the face of legitimate law enforcement/public safety needs and will facilitate cross-border cooperation.

Consideration of public safety issues also is critical with respect to the Commission's proposals to predicate the use of location data on subscriber consent. More and more communications nodes are becoming mobile; as criminals increasingly use mobile communications means, the ability to track their location becomes substantially more difficult. As in the case of traffic data, we urge the Commission to implement a strong harmonized approach among Member States to ensure that its proposals on location data do not make it difficult for investigators to identify and locate criminals who use mobile communication services.

A successful cyber crime investigation also requires that laws are in place that authorize investigators or telecommunications providers to record IP addresses or other traffic information indicating the origin and/or destination of a communication in real time. Many nations and the EU already recognize such an authority, particularly with respect to telephone networks. Thus,

we encourage the Commission to propose EU-wide legislation extending this authority to computer networks. In addition, because real time tracing must be done quickly and seamlessly while a transmission is occurring, the European Union might also consider establishing a single order tracing process that would permit investigators and providers located in different Member States to recognize each other's tracing orders.

We recognize that complying with certain requests for data for public safety purposes may create financial and operational costs for private organizations. Therefore, we support consideration of provisions for compensation of such costs.

- Data Retention and Preservation

As noted previously, access to key electronic evidence is critical to the success of a computer crime investigation. Any rules governing data collection and record-keeping must address these significant public safety considerations, while taking into account other important societal interests, including privacy and the burdens imposed on service providers and other third parties. Careful distinctions must be drawn between data retention - the routine storage by all covered providers of all or large categories of data for a specified period - and data preservation - the storage for a specified period of particular data only if it is already in a particular provider's possession and is relevant to a particular criminal investigation. The United States has serious reservations about broad mandatory data retention regimes and has articulated these reservations in multilateral fora such as the Council of Europe Cybercrime Convention negotiations and the G8.

The United States has taken an approach that neither requires the destruction of critical data, nor mandates the general collection and retention of personal information. Rather, private companies are permitted to retain or destroy the records they generate based upon individual assessments of resources, architectural limitations, security, and other business needs. To protect the public from criminal activity, however, public safety authorities may order a service provider to preserve specified data that is already in the provider's possession if it is relevant to a particular criminal investigation; preservation, however, does not require a service provider to collect data prospectively. The draft Council of Europe Convention contains a similar scheme, reflecting general agreement that, for now, this preservation regime strikes the proper balance between the competing policy interests.

- Anonymity

The United States agrees that anonymity is an extremely difficult and complex issue that requires careful study. In this regard, we are concerned by the Communication's citation from the Declaration of the Ministerial Conference in Bonn on Global Information Networks of the concept, "where the user can choose to remain anonymous off-line, that choice should also be available on-line," which, in our view, fails to capture the very complexities noted in the Communication discussion. In an attempt to create a framework for evaluating identification mechanisms on the Internet, the Bonn Conference and others have compared the Internet with other forms of communications, such as pay telephones and regular mail, which may offer users some degree of anonymity. Of course, the difference between these traditional means of

communication and the Internet is significant, and attempting to solve Internet problems only by drawing analogies to existing technologies will often fail.

The Communication also endorses the recommendation of the Article 29 Data Protection Working Party, which addresses monitoring of newsgroups and possible service provider liability for material made available. The United States has serious reservations concerning the Working Party's recommendation to the extent that it may be read to mandate monitoring by service providers.

- Racism and Xenophobia

The United States is concerned with the Commission's plan to regulate the content of speech on the Internet. As the Commission is aware, in the context of the Council of Europe draft Convention on Cyber Crime the United States had particular concerns in this area and consensus could not be reached on such a provision. Moreover, because of the considerable variation around the world as to what constitutes dangerous or harmful content – which may include religious practices, challenges to government policy, political speech, and even dress – there appear to be significant disadvantages to extensive regulation of content-related speech. We are also concerned that the application of extra-territorial jurisdiction by Member States in such cases can have negative effects on conduct taking place in the United States that is perfectly legal – indeed, constitutionally protected – here. Moreover, in the United States, because restrictions on freedom of expression generally implicate core U.S. domestic values and fundamental human rights, we would be unable to render investigative or prosecutorial assistance to Member States in many content-related cases. Of course, we endorse prohibitions on child pornography because such activities directly endanger children; we also are generally able to assist in content-related cases involving direct threats or incitement of imminent violence. However, we urge the Commission to reconsider its current plans to more generally restrict free expression. We also believe further discussion may be beneficial with respect to some of the difficult jurisdiction and choice-of-law issues that content-related regulations present, and in those areas where wider agreement might be reached.

7.2 Non-legislative Proposals

- EU Forum

The growth of the Internet as a global tool to communicate, engage in commerce, and educate depends on the full participation of all the stakeholders. We believe that the Commission's proposal to establish a forum for representatives from governments and the private sector to share experience and information will assist in building consensus on effective and balanced responses to the problems associated with cyber crime. Although responsibility for public safety must primarily rest with government authorities, industry must take the lead in assuring security and confidence in the systems and networks that it designs, builds, and operates. Consumers and users must also learn to protect themselves and can provide valuable input about their public safety and privacy concerns.

The globalization of our communications networks also requires a global dialogue on the complex issues that face all of us. Policies made in one region of the world necessarily affect the activities in other parts of the world, particularly with respect to the growing problem of transnational crime committed via communications networks. In this regard, the United States reconfirms its desire and commitment to work closely and regularly with the Commission in this process, and would welcome a declaration that the Forum will involve non-EU states as appropriate. We believe the United States and the European Union – both government and the private sector – have much to gain from each other by sharing our experiences and ideas on a regular basis.

- Promoting Security Products

Private industry must take the lead in protecting their networks. Governments, in turn, must avoid inappropriate government regulation that stifles innovation. As noted earlier, we are concerned that some of the European Commission's data protection proposals may make it more difficult for industry to retain the information necessary to monitor and protect its own systems, and share critical information with law enforcement and other industry members.

With respect to the Commission's proposals regarding strong encryption, the United States recognizes the tremendous benefits of encryption to protect privacy and on-line transactions. However, we also must recognize that the same features of encryption technology that are so useful to protect proprietary information and secure communications over the Internet present significant challenges for criminal investigators. While the United States generally supports the use of strong encryption because it prevents crime in the first instance, it is concerned by the use of such technologies by child pornographers, terrorists, and other criminals. The United States government would welcome the opportunity to work with the Commission, private industry groups, and privacy groups to strike a proper balance between these interests.

Technologies that automatically identify the source of a communication may also promote confidence and security by making it easier to identify and locate online criminals. Authentication techniques, including cryptography, are the functional equivalent of a digital seal on a letter, and let the recipient of an electronic communication know who (what machine or person) sent the communication. International Internet standards-setting bodies could serve as a good forum to begin discussing technical standards that would provide for strong authentication. Because communications standards must take into account important public safety concerns, law enforcement should be present to provide input as such standards evolve.

- Taxation

The United States supports the ongoing work being done by the OECD to examine the question of taxation and international e-commerce and believes that EU efforts consonant with efforts in the OECD on this issue would be productive.

- Training and Forensics

Because public safety authorities must take the lead on investigating network and other computer crimes when they occur, and bring those responsible to justice, government officials at the highest levels must commit the resources necessary to recruit and retain high-tech experts, and provide regular technical training and specialized equipment to those experts. Law enforcement agencies need prosecutors, investigators, and forensic analysts dedicated to high-tech crime. As recognized in the G8 and the Council of Europe, at least one investigator or prosecutor with expertise in this field must be available twenty-four hours a day, so that appropriate steps can be taken in a fast-breaking case. Governments must also recognize that as more and more people go on-line, computers will increasingly play some role in all types of criminal activity. Thus, in the future, every law enforcement agent will need to have at least a rudimentary knowledge of obtaining and preserving electronic evidence.

In addition to domestic training, countries should consider coordinated training with other countries so that transnational cases can be pursued quickly. With respect to computer forensics, in particular, it is important to establish compatible forensic standards for retrieving and authenticating electronic data and properly train forensics analysts so that critical evidence is not lost or corrupted. As the Commission knows, the G8, in cooperation with the IOCE, has already begun important work in the area of information technology forensics; therefore, work in other fora should be done in consultation with these existing groups.

Finally, because members of the high-tech industry are the experts on their own systems, government and industry groups should endeavor to develop joint training partnerships. Conversely, because a criminal investigation is dependent on the readiness of technicians at communications companies to access connection data, government must work with industry to insure the availability of trained industry personnel at any time during the day.

- Computer Crime Statistics and Tracking

Although reliable statistics on the number of computer attacks annually are generally lacking, and computer crimes are notoriously under-reported, surveys suggest that the computer systems that support our banking and financial institutions, utility companies, communication and transportation systems, satellite networks, and military establishments are being attacked on a routine basis. A survey conducted by the Computer Security Institute found that over 70% of the 643 corporations surveyed reported network security breaches during 2000. In addition, the CERT (Computer Emergency Response Team) Coordination Center at Carnegie-Mellon University reported a 183% increase in reported incidents between 1998 and 1999, and an increase from 9,859 incidents in 1999 to 15,162 incidents in the first three quarters of 2000.

The damage caused by computer intrusions is more easily quantified. A number of studies suggest that credit card and ATM fraud, account transfers, extortion, telemarketing fraud, and copyright piracy resulted in billions of dollars of losses for individual and corporate victims in 1999 and 2000. According to a study by Meridiem Research, credit card fraud alone cost merchants $400 million in 1999. Even a single malicious act can wreak economic havoc. The creator of the Melissa virus admitted that his virus caused over $80 million in damages in 1999; and damages resulting from last year's "I Love You" virus, and subsequent copycat viruses, are estimated at $6.7 billion in losses to businesses worldwide. In addition, new cyber bank robbers

include Vladimir Levin, who was convicted in 1998 of hacking into a major international bank from Russia and transferring $12 million out of accounts located around the world, and an organized crime group that attempted a $465 million bank heist through the Internet in October 2000. As the Commission recognizes, our networked society also makes it much easier and less risky to commit crimes that directly threaten the safety and health of our citizens, including distribution of child pornography, narcotics trafficking, stalking, threats, and even murder.

But these statistics may represent only the tip of the iceberg. Because of the need for a more systematic measurement, the United States Bureau of Justice Statistics plans to implement a National Computer Crime Statistics (NCCS) Program to gather information on the incidence and prevalence of computer crime offenses, statistical data on the costs and consequences to victims of computer crime, and data on prosecutions, convictions, and sentencing of persons convicted of computer crimes. As a first step, the Bureau of Justice Statistics hopes to implement a statistical series focusing on computer-related crimes that occur against commercial establishments, with subsequent data collections following. The United States encourages other countries to begin collecting data as well so that, ultimately, we can share information and begin to track international trends, set response priorities, and direct our efforts as appropriate.

***