Comments of the United States Government

Communication from the European Commission: "Network and Information Security: Proposal for a European Policy Approach" (COM (2001) 298 (June 6, 2001))[1]

Submitted to the EC on November 21, 2001

I. Introduction

The United States welcomes the opportunity to comment on the European Commission's Communication, "Network and Information Security: Proposal for A European Policy Approach" (COM (2001) 298, June 6, 2001)). The United States government concurs with the European Commission ("the Commission") that the complex issues associated with network and information security are of critical importance. Since our infrastructures largely are owned and operated by members of the private sector, we strongly encourage participation in the development of Commission policy by those interested private parties, including the information technology (IT) industry.

In an effort to highlight certain aspects of the Communication where we consider further thought, clarification, or additional dialogue to be necessary, the United States respectfully submits the following comments. These comments begin with reflection on the urgent need for vigilance in protecting our critical information infrastructures, and continues with some background on basic policies and principles that guide our own work in this area. Following that, we offer specific comments in response to Section 3 of the Communication ("A European Policy Approach") where the Commission has proposed specific actions. We hope these comments will serve as the start of an ongoing dialogue about how best to address the challenges of network security that we both face.

II. Background

As the tragic events of September 11, 2001 make clear, all of our infrastructures are vulnerable to disruption. Disruption can come from acts of terrorists or acts of nature and, when such interruptions occur, they can affect every critical service necessary for governments, economies, and citizens to conduct their essential activities. The terror attacks on the World Trade Center and the Pentagon disrupted and affected networked communications of every nature – emergency services communications; electronic financial transactions; telephone communications between victims, survivors, and loved ones; and Internet access and availability for the latest news on the Web and for e-mail. While no one could have expected an attack on urban centers and civilians of this magnitude, measures of prevention, planning and preparation did mitigate the impact of the attack on our infrastructures. However, to be clear, more must be

[1] A PDF version of the EC's Communication can be found at: http://europa.eu.int/

eur-lex/en/com/cnc/2001/com2001_0298en01.pdf.

done in the future.

Critical infrastructures[2] have been providing services for a long time, and the need for owners and operators of these infrastructures to manage the risks of service disruption has been present throughout this time. Yet only within the last few years have the US and other governments felt it necessary to address the matter of critical infrastructure assurance[3] in a comprehensive manner at the public policy level. The events of September 11 have certainly intensified this focus.

This need for a broader strategy is based on several factors. First, there is a new operational environment for delivering infrastructure services, including increased dependence on information systems and networks; industry deregulation, restructuring and globalization; and increased system complexity, interconnectedness and interdependence. In addition, unique risks and vulnerabilities arising from this new operational environment have prompted governments to develop information infrastructure protection plans. These unique risks include deliberate exploitation by malicious actors, from terrorists on the one hand, to juvenile pranksters on the other, as well as the increased chance of multiple, simultaneous, and cascading disruptions across infrastructure sectors on a regional or national scale (triggered by either malicious or non-malicious events). Finally, as the Communication states, emerging threats (e.g., malicious cyber- and physical acts, natural disasters, human error, or technical malfunction) justify efforts to develop a comprehensive network security strategy.

As part of our efforts in this area, the United States is committed to taking all necessary measures, in partnership with relevant private sector and public sector stakeholders, to assure: (1) the reliable delivery of critical infrastructure services against risks posed by current and emerging threats that would significantly diminish the abilities of the Federal government to fulfill its obligations to provide essential government services (including the performance of missions and functions essential to national security and public health and safety); (2) the ability of state and local governments to maintain order and deliver minimum public services; and (3) the ability of the private sector to ensure the orderly functioning of the national economy, provide essential products and services, and pursue its own business or other purposes. In this partnership, the United States strives to see that cyber- or physical disruption of the operations of any of the critical infrastructures are rare, brief, limited in scope, manageable, and minimally detrimental to the national security, economy, essential government services, and public health and safety. In working with the private sector, we endeavor, whenever feasible, for its

[2] Critical infrastructures comprise those industries, institutions, and distribution networks and systems that provide a continual flow of the goods and services essential to the nation's defense and economic security, the functioning of its government, and the health, welfare, and safety of its citizens. These infrastructures are deemed "critical" because their incapacity or destruction could have a debilitating regional or national impact.

[3] Critical infrastructure assurance is concerned with assuring the readiness, reliability, and continuity of infrastructure services so that they are less vulnerable to disruptions; any impairment is of short duration and limited in scale; and services are readily restored when disruptions occur.

cooperation in this area to be voluntary, and for the overall tenor of these efforts to be industry-led and market-driven. We also strive to give industry the first opportunity to develop technologies, standards, and procedures.

In addition, in this work on critical infrastructure assurance, the United States is guided by a number of imperatives, including:

- partnering between government and industry;
- sharing information within industry sectors, as appropriate and lawful, across industry sectors, and between government and industry;
- promoting market solutions whenever possible;
- securing critical systems and networks nationally and globally;
- assuring services while securing critical cyber- and physical assets;
- developing necessary tools, technologies, and expertise through research & development, education, and training;
- protecting privacy and civil liberties; and
- deterring attacks on critical infrastructures through investigation of incidents and prosecution of those responsible.

Because the impact of regulations and laws in this field so clearly extends beyond the borders of any one country, the United States would like to work closely with the EU as our respective approaches and responses are put in place, so that unintended extraterritorial effects are minimized. Our goal is to ensure compatible and complementary approaches, which will maximize our respective abilities to maintain the security, integrity and smooth functioning of information networks. The United States recognizes that all of these goals cannot be accomplished by any one nation, or group of nations, alone. Therefore, the United States anticipates continuing to work with the Commission, other international groups, and individual countries in areas such as this, where international cooperation is necessary or mutually beneficial.

III. Comments on Proposed Measures in Section 3 of the Communication

(Summary of proposed measures in *italics*.)

3.2 **Awareness raising.** *A public information and education campaign should be launched and best practices should be promoted.*

Comment:

The United States believes that educating users of communication networks and IT professionals is a critical component of any effort to improve the security of networks and information systems. The challenge is not a lack of information, but effectively delivering available information to users and the IT community. The United States supports the recommendation to educate and raise awareness of all stakeholders, and urges the Commission to consult with industry when planning and carrying out this educational program.

The focus of these educational efforts will vary considerably, depending on the audience. However, we believe that universal education for users should begin at a young age. Computer security issues should be incorporated into all introductory computer literacy and computer science curricula, and continued throughout higher education.

Average users should be informed of on-line risks and instructed on ways to protect themselves from intrusions, for example by installing up-to-date anti-virus programs and using firewalls on personal computers. The United States agrees with the Commission that this educational effort must strike a delicate balance by conveying accurate information about Internet risks without exaggeration and in such a way as to minimize unnecessarily alarming the intended audience. In addition, government and industry should raise awareness of acceptable online behavior, distinguishing appropriate Internet use from inappropriate and illegal use, as well as provide guidance on recommended precautions while using the Internet, such as not opening attachments to e-mails sent by persons unknown to the recipient. The United States believes that increasing user awareness will likely contribute to market demand for security products, an additional benefit of the education campaign.

Education of the IT community is equally important. Destructive and malicious viruses frequently spread rapidly across the Internet because of the failure of software providers to fix identified vulnerabilities and of system administrators to fix vulnerabilities and patch their systems against known exploits. IT professionals should be reminded of the need to maintain vigilance in the protection of computer networks through the use of patches and product updates. We further believe that the first line of defense in our shared mission to ensure network security is the development of secure programs and operating systems and we strongly support industry's efforts in this regard. As discussed in more detail below at § 3.7, government can lead the IT community by example in its sustained effort to provide citizens with secure, reliable and functional electronic government services.

At the last United States/European Science and Technology Consultative Meeting which took place earlier this year, the United States extended the Commission an invitation for full membership in the National Colloquium for Information Systems Security Education (NCISSE). The Colloquium established a seat on the board of directors for European participation and plans to include an international track in all future meetings. Founded in 1997, the Colloquium is one of the leading proponents for implementing courses of instruction in information security into higher education. The Colloquium provides a forum for academia, government and industry information security experts to discuss and form needed direction in information security undergraduate and graduate curricula; common requirements; specific knowledge, skills and abilities; certification requirements, and establishment of professional certification boards.[4]

The United States also shares the Commission's interest in encouraging the use of best practices in security. We believe private industry must take the lead in this regard, with input from government and other interested stakeholders. Not only does industry largely design, develop, build, operate and own the infrastructure, software, systems and related technologies

[4] Information about NCISSE can be found at http://www.ncisse.org/.

that connect us, it has the know-how and resources to address its security needs and assess network vulnerabilities. Thus, industry is in the optimal position to develop best practices. Although the United States believes that government should resist unnecessary regulations or restrictions on the Internet that stifle innovation, government should play an active role in encouraging industry-led best practices development and promoting the use of such practices.

Finally, it is worth noting the tension between security measures and functionality. Aggressive implementation of protective measures by users or IT professionals often means sacrificing some degree of functionality. Individual users make choices based on this dynamic. An educational campaign should provide adequate information about risks and protective measures so that the choices made are informed ones.

3.3 **A European warning and information system.** *Member States should strengthen their Computer Emergency Response Teams (CERTs) and improve the co-ordination among them. The Commission will examine together with Member States how to best organise at a European level data collection, analysis and planning of forward-looking responses to existing and emerging security threats.*

Comment:

As the Commission recognizes, an early-warning system and the swift sharing of information about network attacks must be a central component of any network security proposal. Network attacks spread rapidly on the Internet. Effective monitoring and risk assessment are critical to protect computer networks. Because viruses and other malicious code spread with no regard for international borders, there is an urgent need to strengthen early-warning systems worldwide, a need recognized by the Commission. The United States supports strengthening European detection systems.

The United States believes that the private sector should determine its own direction by developing adequate incident monitoring and response schemes and that the government should not mandate or prescribe a particular plan of action. However, governments play the largest role in law enforcement and protecting national security, and therefore should play a strong role with regard to warning and information systems. For example, governments can provide useful input into specific incidents that warrant monitoring and governments can serve as valuable contact points with law enforcement and national security officials. Moreover, government can play a role in helping to determine whether particular monitoring and response schemes are meeting the needs of the public as a whole. In the United States, the National Infrastructure Protection Center (NIPC),[5] located at the Headquarters of the FBI, participates in many of these functions, including disseminating warnings and related information to the private sector.

Equally important is the need to ensure that information is shared in a timely fashion. Open communication among and between industry and the government about how best to ensure

[5] Information about the National Infrastructure Protection Center can be found at http://www.nipc.gov/.

the rapid exchange of information is essential. The United States is acutely aware of this issue because we often look to Europe and Asia for early-warning information due to time differences. The United States supports an ongoing dialogue with the Commission to share experience and information, and to develop a coordinated operational response to attacks and information sharing. As early-warning systems multiply, however, it is essential that incident response teams in the United States and Europe maintain an open dialogue about how best to share information and coordinate responses to network attacks.

By way of comparison, it may be useful to describe the early-warning system in place in the United States. A major reporting center for Internet security attacks is the CERT Coordination Center ("CERT/CC").[6] CERT/CC provides technical assistance and coordinates responses to security compromises, works with other security experts to identify solutions to security problems, and disseminates information to the IT community and the general public. CERT/CC, located at the Software Engineering Institute at Carnegie Mellon University, is funded in part by the federal government and in part by the private sector.

Supplementing CERT/CC's efforts are numerous computer security incident response teams, including the Forum of Incident Response and Security Teams ("FIRST").[7] FIRST is a coalition of individual response teams located throughout the world. Each response team establishes contacts and working relationships with members of its community. FIRST members collaborate on incidents that cross boundaries, and they play a critical role in sharing information about attacks. In addition to the efforts of FIRST, Computer Security Incident Response Teams ("CSIRT") assist in providing support for addressing computer security issues.[8]

CERT/CC, FIRST and CSIRT are only three examples of a complex system of network attack monitoring, information sharing and response teams in the United States. Another is the monitoring and response performed by the National Infrastructure Protection Center. We support effective communication and coordination among the various private response teams and government entities such as the NIPC.

The Communication states, "Once the CERT network is established at EU-level it should be connected to similar institutions world wide, for example the proposed G8 incident reporting system" (Communication, p. 22). Recent meetings of the G8's Subgroup on High-tech Crime and G8 industry conferences in Paris, Berlin, and Tokyo have yielded a number of proposals on information-sharing. For this reason, it is not clear to which specific proposal the Communication refers, and the United States would appreciate clarification on this point.

3.4 **Technology support.** *Support for research and development in security should be a key element in the 6th Framework Programme and be linked to the broader strategy for improved network and information security.*

[6] Information about CERT/CC can be found at http://www.cert.org/.

[7] Information about FIRST can be found at http://www.first.org/.

[8] Information about CSIRTs can be found at http://www/cert.org/csirts/.

Comment:

The United States concurs with the Commission that research and investment in network and information security systems are vital to protect against network attacks. We likewise agree with the Commission on the need to support research in information security. No one entity may have the economic incentive to invest in forms of research and development that have wide applicability to critical infrastructure protection. Information-sharing across borders, where appropriate, increases the breadth of the application of new findings.

The United States is already collaborating with the European Union on a broad range of activities related to the security and dependability of information systems. The collaboration covers both research and development policy, and technical activities. In the policy area, the United States and European Union Task Force on Critical Infrastructure Protection Science and Technology was established in October 1998 to enhance the security of critical infrastructures by identifying, developing, and facilitating technology and policy solutions to existing and emerging threats and vulnerabilities. The Department of State co-chairs this Task Force with a senior EC representative from the Directorate General for Information Society.

Collaboration on technical activities related to information assurance has been in the form of workshops where United States and the Commission have discussed projects of mutual interest. The latest workshop was held in Portugal in February 2001 where principal investigators from the OASIS project sponsored by Defense Advanced Research Projects Agency and the MAFTIA project sponsored by the Commission discussed their respective projects and identified areas of common interest. The security, dependability and survivability of information has also been the subject of conferences sponsored jointly by the U.S. and the Commission. This collaboration has taken the form of cooperative exchanges between U.S. technical agencies and EC research organizations, reciprocal exchange of information on cyber security research programs on an annual basis, visits and exchanges of scientists, and mutual exchanges of scientific and technological information. The U.S. is interested in expanding the collaborative activities with the EU to include closer coordination in identifying and funding projects of mutual interest.

3.5 **Support for market oriented standardization and certification.** *European standardization organizations are invited to accelerate work on interoperability; Commission will continue support for electronic signature and the further development of IPv6 and IPSec, Commission will assess the need for a legal initiative on the mutual recognition of certificates, Member States should review all relevant security standards.*

Comment:

We support the EC's call for better coordination of standardization, and for certification to be strongly endorsed. Deployment of secure, scalable, interoperable, usable, and reliable IT products and services requires the timely development of many coherent and technically sound standards.

We concur with the Commission that it is appropriate for government to encourage broad participation in international standardization efforts. The adoption of standards and specifications – determined by the market with government input and support – is a significant element of any effective network security plan. Since public safety needs play a critical role in this work, and important proposals and funding often come from public bodies, governments should have substantial input in determining broad requirements which will meet overarching public policy goals. At the same time, it should be left to the market to sort out how and through which business practices such requirements are met. And while government will often play a role in the development and promotion of standards and certification of business processes, government funding is not needed in all, or even most, cases.

Whenever practical, we have a strong interest in following a market-driven and industry-led approach, because of the variability of appropriate standards among industry groups and because market and technological forces change so rapidly. When done inappropriately or to excess, imposition of government standards or particular technologies, and prevention of use of tools for testing can be counterproductive, and stifling to innovation.

The United States agrees with the Commission that competing standards and certifications of security business practices create a danger of user confusion, market fragmentation and interoperability complications. While it is innovation and competition in the IT market that drives the IT standards process, competition can lead to deployment problems. We think it significant that it is the innovation and competition in the IT market that creates the problems, and not the IT standards development activities themselves. The solution must be more and better coordination among the IT standards developers.

In the United States, our government participates in this process under guidance from our Office of Management and Budget, and with the particular interest of protecting the national security and national economy. (See, e.g., OMB Circular A-119 <http://www.whitehouse.gov/omb/circulars/a119/a119.html>.) The USG also participates in voluntary industry consensus standards bodies (consistent with OMB Circular A -119) to help ensure its interests (including those of law enforcement) are appropriately represented and considered.

3.6 **Legal framework.** *The Commission will set up an inventory of national measures which have been taken in accordance with relevant Community law. Member States to support free circulation of encryption products. Commission will propose legislation on cybercrime.*

Comment:

We support the Commission's undertaking to develop a common understanding of the legal implications of security in electronic communications. The proposed inventory of national measures that have been taken in accordance with relevant community law will be informative for the Commission, Member States, and our government if this work product can be shared with components of the United States government (e.g., the Department of Justice).

With regard to the Commission's specific proposal for "a legislative measure . . . to approximate national criminal laws relating to attacks against computer systems, including hacking and denial of service attacks" (Communication, p. 26), the United States supports 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 across borders. That cooperation may not be possible, however, if a country does not have the substantive laws in place to facilitate the prosecution or extradition of a perpetrator. The Council of Europe Cybercrime Convention is an important step in this regard.

In addition, 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 cyberspace, 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 and prosecutors need the ability to have service providers preserve for a limited period of time data which already exists within their network architecture and which relates to a specific investigation.[9] Law enforcement relies on providers to preserve these log files, electronic mail, and other records quickly upon notification that such information is necessary for a specific investigation, before such information is altered or deleted. Later access to these historic records, 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. Where service providers are obliged by regulation to destroy traffic data and logs, they would lose their ability to use critical network security methods.

It is for this reason that 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

[9] This procedure, which we refer to as "data preservation," is separate from "data retention," which refers to routine collection and retention for a specific time period of specific categories of data. 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's Lyon Group and Subgroup on High-tech Crime.

Directive. Public safety and law enforcement exemptions, if unimplemented or inconsistently implemented, will lead to inadequate investigative means in some countries and will, in effect, shield cyber criminals from domestic and multi-jurisdictional criminal investigations. Thus, we ask the Commission to work with Member states to ensure that these issues are dealt with effectively and consistently across the EU so that the destruction of critical evidence is not mandated, despite legitimate public safety needs and the need to 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, 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 or impossible for investigators to identify and locate criminals who use mobile communication services.

A successful cybercrime investigation also requires a legal framework that authorizes 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, the United States encourages 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.

Because the impact of legislation in this field so clearly extends beyond the borders of any one country, the United States would like to work closely with the EU as our respective approaches and responses are put in place, so that unintended extraterritorial effects are minimized. Our goal is to ensure compatible and complementary approaches, which will maximize our respective abilities to maintain the security, integrity and smooth functioning of information networks.

Finally, the United States recognizes 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.

3.7 **Security in government use.** *Member States should incorporate effective and interoperable security solutions in their e-government and e-procurement activities. Member States should introduce electronic signatures when offering public services. The Commission will strengthen its security requirements in their information and communication system.*

Comment:

The rise of electronic commerce offers governments exciting opportunities. The many potential benefits of re-designing (or designing) agency processes to use electronic-based processes are apparent: increased efficiency, accessibility, and reliability. At the same time, creating a more accessible and efficient government requires maintaining a secure and reliable information and communications system. It is also critical to ensure public confidence in the security and reliability of the Government's electronic transactions, processes, and systems.

In designing electronic systems, governments should ensure that essential data are available when needed and that the data and the underlying processes are reliable, secure and in compliance with all applicable legal requirements. These protections not only support the twin goals of encouraging similar behavior and potentially influencing the market noted by the Commission, but also fulfill the minimum fiduciary responsibility of government to citizens. In addition, advances in technology, public expectations, and other mandates all require governments to move expeditiously to adopt appropriate electronic processes.

Accordingly, the United States notes with interest proposed actions in the Communication that take advantage of networked communications and other new technologies to encourage effective, efficient and secure interactions between the Commission, Member State governments, and their citizens. We have similar efforts underway in the United States and would like to continue and expand the dialogue that was started under the NTA process to exchange ideas and best practices related to e-government. Under the Government Paperwork Elimination Act (the "GPEA"),[10] federal executive agencies are required, by October 21, 2003, to provide for (1) "the option of the electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper;" and (2) "the use and acceptance of electronic signatures, when practicable." Both the Office of Management and Budget and the Department of Justice have developed guidance to assist agencies in implementing GPEA's requirements. Specifically, the Department of Justice has developed practical guidance on legal considerations related to agency use of electronic filing and record keeping.[11] Among other things, this guidance addresses availability and accessibility, legal sufficiency (i.e., legal validity and enforceability of electronic records and signatures), and reliability for government transactions and related record-keeping.

3.8 **International co-operation.** *The Commission will reinforce the dialogue with international organisations and partners on network and information security.*

Comment:

As the Communication and these comments discuss, threats to networks, and to the critical infrastructures they control, are not confined to any one country or region of the world. Likewise, the need to address network and information security exists in every place where there

[10] Public Law No. 105-277, §§1701-1710 (1998) (codified at 44 U.S.C.A. § 3504).

[11] The Department's guide, which identifies legal issues that agencies are likely to face in converting to electronic processes and provides suggestions on how to address them, can be found at http://www.cybercrime.gov/eprocess.htm.

is Internet connectivity. The United States agrees with the Commission that "addressing security issues require[s] international cooperation." Solutions must be reached though international dialogue and policy coordination.

IV. **Conclusion**

The United States government appreciates this opportunity to comment on the Communication and supports the Commission's proposed action to work with international organizations and partners. The United States hopes to have the opportunity to provide further input on the Commission's work on network security, as that work develops. The United States government remains available to meet with the Commission in Brussels, on these and other issues, as the need arises.

***