THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

LEGISLATIVE AND REGULATORY TASK FORCE REPORT

Penalties for Internet Attacks and Cyber Crime

February 2003

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Protecting the United States' cyber networks, one of its key critical infrastructures, is vital to ensuring the security of the U.S. homeland. Government and industry have made steady efforts to heighten awareness and take action against cyber crimes, and these efforts are likely to continue. The President's National Security Telecommunications Advisory Committee's (NSTAC) Legislative and Regulatory Task Force (LRTF) was tasked with identifying existing legal penalties for prosecuting those committing intentional and malicious attacks on the Internet. It then made recommendations about whether current penalties should be strengthened and/or whether additional penalties were needed. This report represents the NSTAC's recommendations regarding cyber crime laws.

The Computer Fraud and Abuse Act, 18 *United States Code*, Section 1030, is the primary statute for prosecuting cyber crimes. It established penalties for creating computer viruses and conducting malicious Internet attacks, among other provisions. The 107th Congress passed two laws that modified the Computer Fraud and Abuse Act: the USA PATRIOT Act and the Homeland Security Act. These new laws increased existing cyber crime penalties, made it easier to prosecute cyber crimes, and called for a review, and an amendment if necessary, of sentencing guidelines for cyber crimes.

During its deliberations, the LRTF recognized that many of the current cyber crime penalties had been either recently implemented or modified, making it difficult to assess their effectiveness over time. After reviewing current penalties and receiving input from industry and Government experts, the LRTF concluded that existing Federal penalties were adequate for prosecuting cyber crimes. Because it considered current domestic penalties to be sufficient, the LRTF proposed a series of recommendations and suggestions to encourage a well-rounded and proactive approach to preventing and responding to cyber crimes.

The NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472*, Assignment of National Security and Emergency Preparedness Telecommunications Functions* and other existing authority, direct the appropriate departments and agencies, in coordination with industry, to:

- Increase prosecution of cyber crime at the State level;
- Allot additional funds to the States to better train personnel in their jurisdictions on how to prosecute cyber crimes, respond to attacks, and address vulnerabilities;
- Encourage Congress to ratify the Council of Europe (COE) *Convention on Cybercrime,* in conjunction with implementing legislation that provides, among other provisions, for reimbursement of reasonable costs incurred by communications service providers responding to data preservation requests, and encourage other nations to adopt the Convention;

- Work with international counterparts and through multilateral bodies, such as the G-8, COE, European Union (EU), Organization of American States (OAS), and the Asia-Pacific Economic Cooperation (APEC) to:

    - Urge other nations to enact substantive and procedural laws implementing the provisions of the COE *Convention on Cybercrime* or provisions that are at least as comprehensive and that are consistent, wherever possible, with comparable provisions in U.S. law;
    - Encourage other nations to adopt data preservation provisions of the sort set forth in the COE Convention, rather than data retention laws, which require retention *ex ante* of data regarding all communications on a network;
    - Encourage countries to dedicate well-trained and well-equipped personnel to combat cyber crime and designate a 24-hour point of contact on such matters for urgent cross-border investigations; and
    - Encourage better cooperation among nations for locating and identifying cyber-criminals, gathering evidence to bring them to justice, and implementing procedures to more rapidly and effectively prevent and mitigate cyber attacks.

- Encourage companies to implement cyber security best practices by considering the implementation of relevant best practices as a factor in the awarding of Government information technology (IT) contracts.

The NSTAC makes additional suggestions for industry and Government to pursue in order to protect the United States against cyber attacks. These suggestions include coordinating the launch of a nationwide education campaign to increase public awareness of the penalties and consequences for committing Internet attacks. Telecommunications service providers and infrastructure operators should also be encouraged to enter into non-disclosure agreements (NDA) that set a fixed amount of time for mitigating network incidents and vulnerabilities. With sufficient Federal penalties in place to prosecute cyber crime, and additional actions that provide a more well-rounded and proactive approach to fighting cyber crime, the United States can better protect its critical cyber networks from attacks and enhance its national security and homeland defense.

1.0 INTRODUCTION AND CHARGE

To ensure the security of its homeland, the United States must protect its critical infrastructures. One of the country's most vital infrastructures is its cyber network, which enables the operation of key commercial and Government systems that deliver national security and emergency preparedness (NS/EP) communications services. Attacks on the cyber network are steadily increasing and continue to pose a dangerous threat to the U.S. economy and security. Industry sources estimate that in 2001, cyber attacks resulting from malicious code may have caused approximately $13 billion in damages.[1]

Industry and Government have made steady efforts to heighten awareness and take action against cyber crimes. Following the terrorist attacks of September 11, 2001, added attention was given to protecting cyber space, especially from terrorists who might use network attacks to cause widespread damage and outages. In addition, severe Internet attacks such as "NIMDA" and "Code Red" have raised public awareness about the potential damage that cyber attacks can inflict and, in response, many Americans have taken steps to protect their home computer systems. While industry has made progress in securing their networks, company officials say their efforts are sometimes hampered because it is difficult to gauge the financial benefits of making substantial, and hence costly, security upgrades.

On September 18, 2002, the President's Critical Infrastructure Protection (CIP) Board published a draft *National Strategy to Secure Cyberspace*. The draft strategy provides security recommendations for a wide range of Internet users—from small businesses and home users to large enterprises and the Federal Government. The CIP Board plans to update the strategy periodically with input from various groups. In addition, efforts to protect cyber space will likely be a priority at the direction of the new Department of Homeland Security.

As industry, Government, and home users place more of an emphasis on protecting cyber space, it is important to review current legal penalties with regard to cyber crimes, especially those directed at the Nation's NS/EP community. Assessing the effectiveness of the current legal foundation can help policymakers decide whether additional legislation is needed to strengthen the penalties and further secure U.S. cyber assets and the delivery of NS/EP communications.

1.1 Background

During the President's National Security Telecommunications Advisory Committee (NSTAC) XXV Business Session, the Honorable Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the CIP Board, discussed the challenges to Internet security and the serious nature of the threats posed by vulnerabilities within two critical components of the Internet infrastructure—Domain Name Servers (DNS) and the Border Gateway Protocol (BGP). Hackers could exploit such vulnerabilities to create widespread distributed denial of service attacks because Internet protocol (IP) communications occur via

[1] *The National Strategy to Secure Cyberspace*, The President's Critical Infrastructure Protection Board, September 2002, p. 3.

in-band systems. Mr. Clarke urged the NSTAC to examine these vulnerabilities in the Internet architecture. This request led to a discussion about whether to strengthen legislation related to intentional and malicious damage to the Internet and public and private infrastructures/assets through the Internet.

The Internet Security/Architecture Scoping Group initially addressed Mr. Clarke's request. It recommended that the NSTAC's Industry Executive Subcommittee (IES) task the Legislative and Regulatory Task Force (LRTF) to provide recommendations identifying the existing legal penalties for those committing intentional and malicious attacks on the Internet and to determine whether they should be strengthened and/or if additional penalties were needed. This report presents the LRTF's response to those issues.

1.2 Approach

LRTF members, subject matter experts from their respective companies, and Government participants contributed to this effort. Appendix A provides a list of task force members, Government personnel, and other participants. The LRTF also received briefings from officials from the Department of Justice (DoJ) and WorldCom/UUNET on cyber crime laws and computer hacking issues.

1.3 Scope of Study

The LRTF's jurisdiction in this tasking is to identify the existing legal penalties for those committing intentional and malicious attacks on the Internet and recommend whether there should be additional penalties and/or whether existing penalties should be strengthened. The LRTF has addressed this specific tasking. In addition, it has offered recommendations that it believes propose a more proactive and preventative approach to deterring cyber crime. Though some of these recommendations may not be consistent with the LRTF's original tasking, the LRTF believes they may be valuable for preventing cyber crime overall. They also may be useful if NSTAC revisits the cyber crime prevention subject in the future. Because some of the recommendations could be deemed outside of the NSTAC's scope, other Government bodies, such as the Network Reliability and Interoperability Council (NRIC), might also be more suitable for addressing them.

2.0 PENALTIES FOR CYBER CRIME

2.1 Overview of the Legal, Regulatory, and Legislative Environment

The primary statute for prosecuting computer and cyber crimes is Section 1030 of the Computer Fraud and Abuse Act, 18 United States Code, Section 1030. The section sets penalties for creating computer viruses and conducting malicious Internet attacks, among other provisions.

The 107th Congress approved numerous proposals for improving cyber security, including legislation to increase penalties for committing computer crime and to allocate more money for cyber security research and development. Two new laws designed to bolster national security and homeland defense include language to strengthen the Computer Fraud and Abuse Act's cyber crime penalties: the USA PATRIOT Act, which was enacted in October 2001, and the Homeland Security Act, which was signed into law in November 2002.

An official from the DoJ explained that prior to enactment of the USA PATRIOT Act, the Computer Fraud and Abuse Act defined punishable computer "damage" as a loss of at least $5,000 in value during any 1-year period to one or more individuals. The Justice official explained that the Computer Fraud and Abuse Act, as amended by the USA PATRIOT Act, permits losses to several computers from a hacker's course of conduct to be aggregated in order to meet the $5,000 jurisdictional threshold. The USA PATRIOT Act also amended the Computer Fraud and Abuse Act to include a new offense for damaging computers used for national security or criminal justice purposes and increased penalties for hackers who damage such protected computers to as much as 20 years imprisonment for a repeat offense.

The Homeland Security Act amended the Computer Fraud and Abuse Act to authorize life sentences for individuals who knowingly or recklessly commit a computer crime that results in death and 20-year sentences for individuals who knowingly or recklessly commit a computer crime that results in serious bodily injury. The act also directed the United States Sentencing Commission to review its sentencing guidelines for cyber crime and, if appropriate, amend the guidelines to ensure their effectiveness.

2.2 Evaluating the Need for New Penalties

To gain a strong grasp of the current legal environment for prosecuting cyber crimes, the LRTF focused its analysis on the legal statutes that prescribe penalties for cyber abuses. It examined the implementation of key provisions in the Computer Fraud and Abuse Act, as well as other cyber crime laws. In addition, the LRTF reviewed new cyber crime laws, focusing on their changes to current penalties. For a complete summary of Federal cyber crime penalties and recent updates to the law, please see Appendix B.

During its deliberations, the LRTF recognized that many of the current cyber crime penalties and provisions had been either recently implemented or modified. It also acknowledged that recent modifications to the cyber crime laws substantially increased penalties, which would greatly improve the ability to punish for and deter cyber crimes. After assessing the most recent penalties and receiving input from industry and Government experts, the LRTF concluded that the recently modified Federal penalties were adequate for prosecuting Internet attacks because the existing penalties are very strong.

2.3 Additional Findings

The LRTF agreed to report to the IES that sufficient Federal penalties exist to prosecute intentional and malicious attacks on the Internet. Additionally, the LRTF acknowledged that its tasking to address cyber crime penalties was narrow in scope. It recognized that taking certain actions, in addition to having sufficient Federal penalties, would offer a more well-rounded, proactive, and preventative approach to deterring cyber crime.

2.3.1 State Law

The LRTF acknowledged the importance of having sufficient legal penalties in place not only at the Federal level but also at the State level. State penalties for cyber crimes should be consistent with Federal penalties and must be strong enough to make the threat of State prosecution deter cyber crime throughout the Nation. In addition, States should have the necessary resources to train their personnel on how to address network vulnerabilities and respond effectively to cyber attacks. States should also better educate the appropriate local officials on how to prosecute cyber crimes in their jurisdictions. Having sufficient penalties in place at the State level and having citizens who know how to mitigate and respond to attacks will help secure the Nation's cyber infrastructure.

2.3.2 International Law

The vast majority of Internet attacks have an international component, making prosecutions of cyber crimes difficult because they often fall within the jurisdiction of other countries. While the LRTF believes that existing Federal laws are sufficient for prosecuting domestic cyber crimes, these laws are ineffective for prosecuting attacks that are generated outside of the United States. Therefore, having positive diplomatic relations with other countries is critical to U.S. cyber crime efforts, as the nature of the relationship often determines the level of cooperation for prosecuting a foreign hacker.

There are four major areas of importance to the United States when working with other nations on cyber crime. First, other nations should implement strong anti-hacking laws to make it easier to prosecute criminals. Strong procedural laws in other countries also facilitate the retrieval of evidential information for cyber crime investigations. Second, countries should have dedicated computer crime personnel who are well trained, well equipped, and available around-the-clock to respond to cyber incidents. It is beneficial if these personnel are able to identify the sources of the Internet attacks and capture data immediately. Third, it is important to have a mechanism for

locating and identifying the source of an attack that originates from abroad and preserving that evidence. Finally, it is important to be able to effectively gather evidence from other nations to enable prosecution for an attack with an international component. Performing computer forensics, such as authenticating digital pictures and e-mails, would help in the prosecution of cyber criminals. Presently, it is difficult to gather such evidence from abroad and to secure citizens from other countries to testify against cyber criminals because of the distances they need to travel to do so. Ideally, it would be beneficial to conduct investigations abroad as they are conducted in the United States.

In addition, the disparate approaches to the way computer data is handled overseas continues to hamper U.S. cyber crime investigations. Some nations mandate the retention of data for a set period of time, such as 90 days. Data retention laws require retention *ex ante* of data regarding all communications on a network. Other countries prefer to provide for preservation of data once an investigation has begun or restrict its transfer across national boundaries.[2] Some nations also require companies to destroy certain data after a period of time. Data destruction is common in some European Union (EU) member states, particularly in those that place a high premium on protecting the privacy of personal data. This lack of consistency among international data laws often makes it difficult for the United States to gather cyber crime evidence. Encouraging other nations, particularly the EU member states, to eliminate data destruction requirements and to adopt stronger and more consistent data preservation laws—instead of data retention laws—would create greater legal consistency at an international level and would be helpful to U.S. efforts. Communications service providers generally accept the need for law enforcement to request that data associated with specific accounts or communications be preserved, but these providers should receive reimbursement for complying with these requests.

There are several international bodies with which the U.S. can cooperate to gain support for international cyber crime initiatives. The G-8 is considered the most effective body for cooperating on cyber crime efforts. Despite having only eight members, the G-8's focus on fighting cyber crime and the frequency of meetings among the Heads of State have assisted the U.S.' international cyber crime initiatives. In addition, the Council of Europe (COE) consists of 43 countries and is designed to facilitate international cooperation. On November 23, 2001, the COE adopted its *Convention on Cybercrime* (ETS no. 185). The Convention is the first international treaty on cyber crimes with the goal of pursuing a common criminal policy to protect society against cyber crimes. It seeks to achieve this goal by harmonizing domestic criminal substantive and procedural laws for gathering evidence and prosecuting cyber crimes and by establishing a regime for international cooperation. It also encourages a policy of data preservation. Several nations, including the United States, have signed the treaty. However, the United States and several other countries have not ratified the treaty. In that the United States signed the COE *Convention on Cybercrime* on November 23, 2001, the NSTAC recommends the

[2] The G-8 has defined data preservation as when: (a) upon lawful request by a competent authority, (b) based on the facts of a specific case, (c) specific historical data can be preserved to prevent its deletion, (d) pending issuance of a lawful demand from a competent. According to the G-8 definition, "preservation" does not include the prospective collection of data and does not obligate a service provider to generate data that it does not routinely require for lawful business practice.

Administration urge Congress to ratify the treaty at the earliest practical date.[3] In addition, Congress should ratify the treaty in conjunction with implementing legislation that provides, among other provisions, for reimbursement of reasonable costs incurred by communications service providers responding to data preservation requests.

Federal agencies should also work with international counterparts and through multilateral bodies, such as the G-8, COE, EU, Organization of American States (OAS), and the Asia-Pacific Economic Cooperation (APEC) to encourage other nations to effectively address cyber crime. Specifically, they should urge other nations to enact substantive and procedural laws implementing the provisions of the COE *Convention on Cybercrime* or provisions that are at least as comprehensive and that are consistent, wherever possible, with comparable provisions in U.S. law. United States officials should encourage other nations to adopt data preservation provisions, such as those set forth in the COE Convention, instead of data retention laws. They should also encourage countries to dedicate well-trained and well-equipped personnel to combat cyber crime and designate a 24-hour point of contact for urgent cross-border investigations. Agencies should also encourage better cooperation among nations for locating and identifying cyber-criminals, gathering evidence to bring them to justice, and for implementing procedures to more rapidly and effectively prevent and mitigate cyber attacks.

2.3.3 Cyber Security Best Practices

The LRTF recognizes that encouraging the private sector to improve cyber security is critical to developing a well-rounded, proactive, and preventative approach to deterring cyber crime. Private sector networks are vital to keeping the U.S. economy running smoothly. Companies should implement common best practices for computer security that include concrete ramifications for abuses rather than lenient consequences. The Government could encourage companies to implement cyber security best practices by considering the implementation of relevant best practices as a factor in the contracting process of Government information technology (IT) contracts. There are several ways companies can implement common best practices, such as keeping current with patches and anti-virus software, understanding perimeters/filters and firewalls, and scanning systems periodically. In addition, the NRIC and the National Institute for Standards and Technology (NIST) are developing sets of cyber security best practices that are available for consideration. With encouragement from the Government, companies could enhance their security practices, which can better secure Internet systems across the nation.

2.3.4 Information Exchange

The majority of the Nation's critical infrastructures are owned and operated by the private sector. Therefore, it is important that the private sector share information about vulnerabilities in these systems with each other and with the Government. The recently enacted Homeland Security Act includes a provision that would protect voluntarily shared critical infrastructure information from

[3] The Council of Europe Website on the *Convention on Cybercrime,* http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/Convention/The_Convention.asp#TopOfPage.

public disclosure under the Freedom of Information Act (FOIA).[4] This provision aims to better protect sensitive information from falling into the hands of those who would exploit infrastructure vulnerabilities and help protect companies from having such information used against them. This provision should also help encourage the private sector to share information about the Nation's critical infrastructures.

In addition to the FOIA modification, the Homeland Security Act contains a provision that limits legal liability for sharing critical infrastructure information. Section 214 states that shared critical infrastructure information "shall not … be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith." In addition, Section 861-865 contains a provision that limits legal liability of companies that provide "qualified anti-terrorism technologies" to the Federal Government.[5] While this provision does not specifically address potential liability issues when companies share vulnerability information with the Government, this protection is important for shielding anti-terrorism technology vendors.

In October 1997, the President's Commission on Critical Infrastructure Protection (PCCIP) published a report that detailed the growing capability to exploit information infrastructures and underscored the need for establishing information-sharing structures within the Government and the private sector. Building on the commission's recommendations, the White House issued Presidential Decision Directive (PDD) 63 in May 1998, which called for the creation of public-private partnerships to help eliminate vulnerabilities in critical infrastructures.

To advance those efforts, the LRTF has examined potential barriers to voluntary information sharing related to NS/EP communications, critical infrastructure protection, or other similar subjects. Previous LRTF reports have identified an array of barriers, including the potential damage to companies if their trade secrets and proprietary information are released; impediments that companies perceive might arise from antitrust and unfair business practices; liability concerns; and State government liability and disclosure concerns.[6] Despite new provisions in the Homeland Security Act to encourage the sharing of critical infrastructure information, additional barriers to information sharing may still exist. For example, the LRTF notes that private contractual relationships in non-disclosure agreements (NDA) can also hinder information sharing. The LRTF will continue to examine whether additional barriers to information sharing remain, especially with regard to liability and antitrust concerns.

2.4 Suggestions for Industry and Government

The LRTF also formulated a series of proactive and preventative suggestions for the Government and industry to help deter cyber crime. Fundamental to that effort is making the culture of

---

[4] The Homeland Security Act of 2002, Subtitle B, "Critical Infrastructure Information," Section 214.

[5] The Homeland Security Act of 2002, Subtitle G, "Support Anti-terrorism by Fostering Effective Technologies Act of 2002," Sections 861 through 865.

[6] Telecommunications Outage and Intrusion Information Sharing Report, NSTAC Legislative and Regulatory Group, June 1999, Section 4.0, "Potential Legal Barriers to Information Sharing," p. 24.

computer hacking more unattractive to potential script kiddies and hackers. To that end, the LRTF suggests that industry and the Government support already existing initiatives to develop nationwide educational campaigns, such as Stay Safe Online (SSOL), to increase public awareness of the penalties and consequences for committing Internet attacks.

Industry should also seek more contractual flexibility to report vulnerabilities and threats. The LRTF suggests that telecommunications and infrastructure providers enter into NDAs that set a fixed amount of time for mitigating network incidents and vulnerabilities. Such NDAs should permit vulnerabilities to be released to the proper authorities if an incident is not adequately addressed within the specific timeframe. The LRTF notes that the CERT® Coordination Center is currently studying a related issue. Further, the LRTF suggests that contracts between infrastructure operators and Internet service providers follow a structure that allows infrastructure providers to inform authorities about an attack or vulnerability if a certain percentage of their infrastructure is threatened.

3.0 CONCLUSIONS

The LRTF concludes that sufficient legal authority exists in the United States to penalize those who commit cyber crimes and to act as a deterrent for those considering committing such acts. In addition, the LRTF recognizes that having sufficient legal penalties in place cannot completely stop cyber crimes altogether and that a more proactive and comprehensive approach to curbing cyber crime is necessary to protect the United States' critical networks. While addressing broader issues may fall outside the LRTF's scope for this tasking, the LRTF believes that providing additional recommendations, such as those included in this report, may encourage a well-rounded and proactive approach to preventing and responding to cyber crimes.

4.0 RECOMMENDATIONS

NSTAC Recommendations to the President

The NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472*, Assignment of National Security and Emergency Preparedness Telecommunications Functions* and other existing authority, direct the appropriate departments and agencies, in coordination with industry, to:

- Increase prosecution of cyber crime at the State level;

- Allot additional funds to the States to better train personnel in their jurisdictions on how to prosecute cyber crimes, respond to attacks, and address vulnerabilities;

- Encourage Congress to ratify the COE *Convention on Cybercrime,* in conjunction with implementing legislation that provides, among other provisions, for reimbursement of reasonable costs incurred by communications service providers responding to data preservation requests, and encourage other nations to adopt the Convention;

- Work with international counterparts and through multilateral bodies, such as the G-8, COE, EU, OAS, and APEC to:

  - Urge other nations to enact substantive and procedural laws implementing the provisions of the COE *Convention on Cybercrime* or provisions that are at least as comprehensive and that are consistent, wherever possible, with comparable provisions in U.S. law;
  - Encourage other nations to adopt data preservation provisions of the sort set forth in the COE Convention, instead of data retention laws, which require retention *ex ante* of data regarding all communications on a network;
  - Encourage countries to dedicate well-trained and well-equipped personnel to combat cyber crime and designate a 24-hour point of contact on such matters for urgent cross-border investigations; and
  - Encourage better cooperation among nations for locating and identifying cyber-criminals, gathering evidence to bring them to justice, and for implementing procedures to more rapidly and effectively prevent and mitigate cyber attacks.

- Encourage companies to implement cyber security best practices by considering the implementation of relevant best practices as a factor in the award of Government IT contracts.

APPENDIX A

TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

Telcordia Technologies	Ms. Louise Tucker, Chair
Lockheed Martin	Mr. Gerald Harvey, Vice Chair
AT&T	Mr. Harry Underhill
BellSouth	Mr. Shawn Cochran
Boeing	Mr. Robert Steele
Cisco Systems	Mr. Brian O'Connor
CSC	Mr. Guy Copeland
Dell Computers	Mr. John Lavorato
EDS	Mr. Dale Fincke
Lucent Technologies	Ms. Gena Ashe
Microsoft	Mr. Bill Guidera
Qwest Communications	Ms. Jane Kunka
Raytheon	Mr. Thomas O'Connell
Rockwell Collins	Mr. Ken Kato
SBC Communications	Ms. Rosemary Leffler
Sprint	Mr. Michael Fingerhut
TRW	Mr. Tim Nagle
Unisys	Ms. Gayle Cozens
VeriSign	Mr. Michael Aisenberg
Verizon Communications	Ms. Ernie Gormsen
WorldCom	Ms. Cristin Flynn

OTHER PARTICIPANTS

CSC	Mr. Daryl Savage
Dell Computers	Mr. Paul Brownwell
George Washington University	Dr. Jack Oslund
Lockheed Martin	Mr. Larry Duncan
Qwest Communications	Mr. Jon Lofstedt
Unisys	Mr. Fred Tompkins

GOVERNMENT PARTICIPANTS

DISA Counsel	LtCol Keith Alich
OMNCS Counsel	Mr. Paul Schwedler

BRIEFERS

DOJ	Mr. Todd Hinenn
DOJ	Mr. Christopher Painter
WorldCom/UUNET	Mr. Brian Gemberling
WorldCom/UUNET	Mr. Chris Morrow
WorldCom/UUNET	Mr. Rob Rigby

APPENDIX B

CYBER CRIME PENALTIES CHART

FEDERAL CYBER CRIME LAWS

Law	USA PATRIOT Act Provisions	Homeland Security Act Provisions
18 U.S.C. § 1030, "The Computer Fraud and Abuse Act." **Fraud and Related Activity in Connection with Computers** Section 1030 includes penalties for crimes such as creating viruses and malicious attacks and creates penalties for someone who knowingly intends to cause damage.	• Increase penalties for hackers who damage protected computers (a maximum of 10 years for first offenders and a maximum of 20 years for repeat offenders) • Clarify the *mens rea* required for such offenses to make explicit that a hacker need only intend damage, not a particular type of damage • Add a new offense for damaging computers used for national security or criminal justice • Expand the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce • Count state convictions as "prior offenses" for purpose of recidivist sentencing enhancements • Allow losses to several computers from a hacker's course of conduct to be aggregated for purposes of meeting the $5,000 jurisdictional threshold	• Authorizes life sentences for individuals who knowingly or recklessly commit a computer crime that results in death • Authorizes 20-year sentences for individuals who knowingly or recklessly commit a computer crime that results in serious bodily injury • Directs the U.S. Sentencing Commission to review and amend federal sentencing guidelines where appropriate for computer crimes involving fraud and access to protected or restricted data • Such guidelines would reflect the need for a deterrent and would require consideration of any resulting losses and violations or disruptions of privacy, national security, public health or safety
18 U.S.C. § 1029 Fraud and Related Activity in Connection with Access Devices	Using unauthorized access devices to obtain anything of value over $1,000 or obtaining unauthorized access to telecommunications services could result in: • A fine and/or up to 15 years imprisonment • Second offenses can result in up to 20 years imprisonment	
18 U.S.C. § 1361 **Penalties for injuring or**	• If the damage or attempted damage to such property exceeds the sum of $1,000, it may result in a fine and/or up to 10 years imprisonment	

committing any depredation against Government property or contracts	• If the damage or attempted damage to such property does not exceed the sum of $1,000, it may result in a fine and/or up to 1 year imprisonment	
Law	**USA PATRIOT Act Provisions**	**Homeland Security Act Provisions**
18 U.S.C. § 1362 **Communication Lines, Stations, or Systems**	Targets damage to or interference with property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States Government, or used or intended to be used for military or civil defense functions of the United States • Includes no minimum monetary damage requirement • Penalties include a fine and/or up to 10 years imprisonment	
18 U.S.C. § 2511 Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited	• Penalties include a fine and/or up to 5 years imprisonment	• Removes special penalty treatment for first time offenders who intercept a cellular phone call. Permits up to 5 years of jail time for first time offenders who intercept a cellular call
18 U.S.C. § 2701 Unlawful Access to Stored Communications Intentional access without authorization of a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a	If the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, penalties include: • First-time offenders may be fined or subject to imprisonment for up to 1 year • Repeat offenders may be imprisoned for up to 2 years • If the unlawful access is not for any of the stated purposes, then the offender may be fined or subject to imprisonment for up to 6 months	• Expands the list of disfavored purposes to include unlawful access in furtherance of any criminal or tortious act that violated any law • Raises the maximum criminal penalties from 1 to 5 years of imprisonment for first offenders and from 2 years to 10 years for repeat offenders • Maximum penalties for other violations are set at 1 year for first offenders and 5 years for repeat offenders

wire or electronic communication while it is in electronic storage.		