AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 106–838

"CYBER ATTACK: IMPROVING PREVENTION AND PROSECUTION"

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

ON

EXAMINING HOW TO COMBAT CYBER ATTACKS BY IMPROVING PREVENTION AND PROSECUTION

SCOTTSDALE, AZ

APRIL 21, 2000

Serial No. J–106–79

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
69–335 WASHINGTON : 2001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

STROM THURMOND, South Carolina
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JOHN ASHCROFT, Missouri
SPENCER ABRAHAM, Michigan
JEFF SESSIONS, Alabama
BOB SMITH, New Hampshire

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
ROBERT G. TORRICELLI, New Jersey
CHARLES E. SCHUMER, New York

MANUS COONEY, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Minority Chief Counsel*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

JON KYL, Arizona, *Chairman*

ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
MIKE DEWINE, Ohio

DIANNE FEINSTEIN, California
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin

STEPHEN HIGGINS, *Chief Counsel and Staff Director*
NEIL QUINTER, *Minority Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Kyl, Hon. Jon, U.S. Senator From the State of Arizona	1

CHRONOLOGICAL LIST OF WITNESSES

Panel consisting of Janet Napolitano, Attorney General, State of Arizona; and Guadalupe, Gonzalez, Special Agent In Charge, Phoenix Field Investigation, Federal Bureau of Investigation	3
Panel consisting of David W. Aucsmith, chief security architect, Intel Corp.; and Jose Grando, senior manager, Ernst & Young LLP, Houston, TX	89

ALPHABETICAL LIST AND MATERIAL SUBMITTED

Aucsmith, David W.:	
Testimony	89
Prepared statement	93
Gonzalez, Guadalupe:	
Testimony	66
Prepared statement	71
Granado, Jose:	
Testimony	102
Prepared statement	104
Napolitano, Janet:	
Testimony	3
Prepared statement	5
Letter from the Attorney General	11
Summary	13
Computer Crimes Act of 2000	15
Attorney General's Website	54
News Articles	57

"CYBER ATTACK: IMPROVING PREVENTION AND PROSECUTION"

FRIDAY, APRIL 21, 2000

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM,
AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Scottsdale, AZ.

The subcommittee met, pursuant to notice, at 9 a.m., in City Council Chambers, Scottsdale, AZ, Hon. Jon Kyl (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. This hearing will please come to order.

Let me first welcome everyone to this field hearing of the Subcommittee on Technology, Terrorism, and Government Information of the U.S. Senate Judiciary Committee. It is encouraging to see so many people who are interested in this critical subject. Before we begin, I want to thank the Mayor of Scottsdale, Sam Campana, for hosting us here at the Scottsdale City Council chambers and for the assistance of Peggy Carpenter from the city of Scottsdale, who helped set up this hearing. I also want to thank Ed Denison from the Arizona Software Association for his assistance in spreading the word about the hearing, and, finally, to say hello to the people watching this hearing on the city of Scottsdale's Cable Television channel.

The danger from cyber attack has recently received a lot of attention. The denial-of-service attacks against popular Internet sites like Yahoo, eBay, and CNN and the arrest earlier this week of a Canadian teenager in the case brought home to Americans just how vulnerable we are. This is the seventh hearing I have held on the subject in the past 3 years, and it won't be the last.

In examining how to combat cyber attacks, it is important to reflect on how the Information Age is rapidly transforming our society. Today, virtually every key service is dependent upon computers—from electrical power grids, to phone systems, air traffic control, banking, military early-warning networks. The list goes on and on. Unfortunately, most of these critical computer networks were not designed with good security measures in mind.

America's increased dependence on computer networks must also be viewed in context of our changing role in the post-cold war world. The United States is the world's only superpower, and our armed forces enjoy technological superiority on the battlefield. I sit

on the Senate Intelligence Committee, and I receive a lot of briefings from the CIA and others about threats facing our country. The overriding trend in these briefings is that nations and terrorist groups that are hostile to our interests are increasingly choosing not to confront our military strengths directly—that is, by trying to field fleets of advanced fighter planes or aircraft carriers on a par with ours—but, rather, are seeking to exploit our vulnerabilities, looking hard for our Achilles heel. As the ancient Chinese military strategist Sun Tzu said, "You can be sure of succeeding in your attacks if you only attack places which are undefended."

China's current military strategists appear to have taken this lesson to heart. A recent article in the official Liberation Army Daily stated that China is considering creating a fourth branch of the military for information warriors and said "Internet warfare" should be equated with air, land, and sea combat operations.

Russia is another country of concern in this area. Last year, a series of widespread intrusions were detected on computer networks operated by the Defense Department, other Federal agencies, and the private sector. The FBI traced these intrusions to Russia in an operation dubbed Moonlight Maze. According to the FBI, the attacks resulted in the theft of vast quantities of unclassified, but still sensitive information about defense technological research matters. Although the details of the case are classified, according to Newsweek Magazine, the primary suspects in the intrusions, which have since terminated, are "crack cyber spooks from the Russian Academy of Sciences, a government-supported organization that interacts with Russia's top military labs." And Russia and China are not the only countries of concern. According to the National Security Agency, over a dozen countries are working on information warfare techniques.

U.S. military planners have also begun to try to assess how cyber attacks could affect our military's performance and to take steps to close those vulnerabilities. In 1997, the Joint Chiefs of Staff conducted an exercise called Eligible Receiver to find out how easy it would be for an enemy to attack U.S. military communication systems and other critical infrastructures. During the exercise, a small team of 2 dozen people used readily available computer hacking tools to attack the military's critical infrastructures and within 4 days crippled our ability to respond to a simulated crisis in the Pacific theater. They also broke into networks that control the electric power grid for the entire United States.

In addition to being conscious of the threat from foreign countries and the need to take steps to improve the security of the critical computer networks, we need to combat computer hacking by criminals here in the United States, which can also have very serious consequences. The number of computer crimes is rapidly increasing, and we need to be sure that Federal, State, and local law enforcement agencies have the tools they need to investigate and prosecute violators.

Catching and punishing those who commit cyber crimes is essential for deterring future attacks. When a cyber attack occurs, it is not initially apparent whether the perpetrator is a mischievous teenager, a professional hacker, a terrorist group, or even a hostile nation. Law enforcement must be equipped with the resources and

authorities necessary to swiftly trace a cyber attack back to its source and appropriately prosecute criminals.

Finally, it is important to recognize that private companies own and operate the vast majority of the computer networks used to operate our critical infrastructure. We must raise awareness in industry about cyber threats, encourage companies to take responsible steps to protect themselves, and remove roadblocks to effective industry cooperation. For example, protection from attack necessitates that information about cyber vulnerabilities and threats be communicated among companies and with government agencies. Antitrust laws that were created to prevent collusion among competitors in an industry need to be updated to allow companies to cooperate in establishing good cyber security. Furthermore, the Freedom of Information Act may need to be updated to encourage companies to share information with the Federal Government. Communication is critical for protection, and these roadblocks need to be removed.

Our witnesses are well suited to address these issues. On our second panel, David Aucsmith, the Intel Corporation's top security specialist, will discuss some of the trends and challenges in cyber security, and Jose Granado, a senior manager of Ernst & Young, will conduct a live computer hacking demonstration. Guadalupe Gonzalez, the special agent in charge of the FBI's Phoenix Office, will provide the Federal law enforcement perspective on cyber crime.

Before we hear from these three experts, I would like to introduce our first witness, Arizona Attorney General Janet Napolitano. Ms. Napolitano has served as attorney general since January 1999, and prior to her election to this post, she served for over 4 years as the U.S. attorney for Arizona.

Attorney General Napolitano, thank you very much for testifying at today's hearing. Your full statement and that of all of the witnesses will be included in the record, and I would invite you to make any summary remarks at this time.

PANEL CONSISTING OF JANET NAPOLITANO, ATTORNEY GENERAL, STATE OF ARIZONA; AND GUADALUPE GONZALEZ, SPECIAL AGENT IN CHARGE, PHOENIX FIELD INVESTIGATION, FEDERAL BUREAU OF INVESTIGATION

STATEMENT OF JANET NAPOLITANO

Ms. NAPOLITANO. Thank you, Mr. Chairman, and thank you for inviting me to be here today and for your long-time interest in the cyber area. You have truly been a national leader in this regard, and we are grateful.

Arizona is one of the leading States, I believe, in prosecuting computer crime. In the Attorney General's office, we have established a Technology Crimes Unit. The head of that unit is with me today, Gail Thackery, who is one of the Nation's leading prosecutors in this emerging area.

We also now have one of the most comprehensive computer crime statutes in the country that was passed by the legislature this past session, was recently signed into law by Governor Jane Hull, and had broad bipartisan support.

Let me, if I might, divide my summary remarks into three brief categories, and I understand my full statement will be admitted into the record. But the three categories are what kinds of things we're seeing at the State level in Arizona, what is in our cyber crime legislation that supports and augments what is in some of the proposed Federal legislation, and, finally, what we as State prosecutors would like to see from the Federal Government.

But, very briefly, lest we think that all cyber crime takes place internationally or in cyberspace somewhere else, we have a great deal of it here in Arizona, and it really doesn't matter whether you are in urban Arizona or rural Arizona. Anywhere you have a PC you have the potential of a cyber crime.

Currently, we have cases in our office pending involving the five following kinds of cyber crime: cyber stalking, online school threats, infrastructure attacks and hacker offenses, fraud—in fact, in our Consumer Fraud Division in the Attorney General's office, we have now created a separate way to track the Internet fraud cases so that we can follow the trend line more accurately as to what kinds of fraud we are seeing on the Internet—and child sexual exploitation cases. We currently have task forces involving child sexual exploitation in Tucson and Phoenix, and our office is helping Arizona post the training agency for law enforcement train investigators and prosecutors in this area.

So you can see we have quite a panoply of different types of computer crimes. Some are old kinds of crime committed in new ways, i.e., fraud. Some are new crimes that we could not have imagined 20 years ago.

To deal with this, our office proposed the Computer Crime Act of 2000 in Arizona, and briefly, Senator, that statute, which is attached to part of my testimony, has six parts. One is cyber terrorism, and it raises the penalties for disrupting operations of things like utilities, emergency services, medical institutions, traffic control and the like.

It contains cyber tools for law enforcement. For the first time, for example, our office has the ability to seek the source of e-mails through desk subpoenas rather than having to go continually to court, a concept I think that the FBI is supporting federally.

It has sections on forgery, fraud, and theft, and acknowledges that people have online identities that themselves can be the subject of the theft of identity.

It has a new felony for cyber stalking because the current laws were not adequate to deal with the prosecution of those offenses.

It has a felony for computer use and disruption. The denial of service attacks you mentioned in your opening statement are now felonies in Arizona. I think we are one of the few jurisdictions in the country that actually has that.

And, finally, it has provisions related to child pornography on the Internet, and it adds the offense of luring—l-u-r-i-n-g—meaning that the offense of sexual solicitation of a minor is committed with the solicitation itself. It doesn't require any further act in furtherance of the crime of meeting the minor in order to be able to charge the higher felony. We make the solicitation itself, the luring, a crime on the Internet. So that is the new Arizona bill.

Now, we have a Technology Crimes Unit, as I mentioned, and I might like to say that this year the legislature, under the leadership of Representative Jim Wyers from the northwest part of the valley, passed a bill that provides some monetary resources both to the Attorney General's office and to the Department of Public Safety to help us meet the increasing need. And as good a bill as that is, it is only a first step in terms of the resources that State and local prosecutors are going to need. The chief thing we need from the Feds, if I can use the nickname, right now is training and resources.

Attorneys, investigators, and prosecutors with computer skills are in incredible demand. We are unable to hire people with this expertise because State and local public salaries simply are not competitive in the current marketplace. That means what we need to do and what we are doing is training people who are already in public service on how to deal with these new kinds of crime. That means training is very, very key. It is expensive, and it also requires equipment that is continually updated to match what is out there in the field.

As I have already indicated, the bulk of prosecuting these crimes, the bulk of these crimes, be it identity theft, be it a child pornography case, be it a luring case, are going to end up being prosecuted by State and local authorities because that is where the bulk of prosecutions in this country occurs in any area. And the same is holding true in cyber crime.

So we would like to emphasize the need for training resources, and there are existing vehicles already in place to deliver that training, both through the National District Attorneys Association and the National Association of Attorneys General. NAAG, by the way, has made cyber crime one of its top priorities, and I would ask that the Senate and that you consider how we make those training resources available on a continual basis, not a one-time thing but continual, because the technology keeps changing.

The other idea I would like to offer to you, Sir, is something that is reminiscent of what the Senate and the Congress did in the 1970's when they provided seed money to Attorneys General to open up or to start antitrust units or economic competition units within their offices to handle those kinds of cases. Seed money for every Attorney General to have a cyber crime unit such as we have in Arizona, or to build on one if they already have one, I think would provide a very big bang for the buck in the sense of expanding our reach, expanding our prosecutorial resources, and expanding what we can do working with these new technologies to make sure and to ensure that basic law enforcement is being carried out, be it in cyberspace or be it on the ground.

Thank you very much.

[The prepared statement of Ms. Napolitano follows:]

PREPARED STATEMENT OF JANET NAPOLITANO

Mr. Chairman, thank you for the opportunity to address your subcommittee today. As the Attorney General of Arizona, I am here to report on our state's activities in combating and prosecuting cybercrime. Cybercrime is an emerging issue in law enforcement as an increasing number of crimes are committed using computers and other technologies. In fact, while we have seen a decline in violent crime, cybercrime has increased exponentially. As crime migrates to the Internet and other frontiers

of technology, law enforcement must be adequately prepared to apprehend and prosecute the criminals.

Instead, law enforcement has had a difficult time keeping up with cybercrime. Laws have been found to be inadequate in dealing with new technologies. The speed with which technology advances demands rapid and innovative solutions to complex problems. Lastly, there is a desperate lack of resources for cybercrime law enforcement. There are three issues I want to discuss today—legislation, emerging issues in cybercrime and current challenges facing law enforcement.

ARIZONA LEGISLATION—THE COMPUTER CRIMES ACT OF 2000

The Office of the Attorney General drafted the Computer Crime Act of 2000, which was sponsored and passed by a bi-partisan coalition of legislators. HB 2428, recently signed into law by Governor Jane Dee Hull, is designed to better protect Arizona citizens from cybercrime, which is a threat to private citizens, public infrastructure, businesses, and government, as these incidents prove:

• In 1998 a computer user in Arizona hacked his way onto a billing database of a public utility, looking to cancel someone's account. Once in the system, he gained high-level access to the canal controlling system, putting the system at serious risk.

• Just this past year, a young man, angry at his ex-girlfriend, posted pictures of her and assumed her identity on the Internet. Through sexually explicit e-mail with other users, he put the young woman in great danger to potentially become a victim of sexual assault or worse by inviting people to her home and workplace.

• Phoenix man hacked into the computer of an Internet Service Provider in Canada and crashed the server, disabling the entire network, including all e-mail services, for a week. Numerous businesses and individuals lost valuable information, time and money.

There are six parts to this legislation:

Cyberterrorism

We must use every means available to crack-down on attacks on our high-tech infrastructure. This section raises judicial penalties for disrupting operations of utilities, emergency services, medical institutions, traffic control, etc.

Cybertools for law enforcement

Cybertools strengthen law enforcement's ability to preserve electronic evidence and to trace rapidly criminal activity on the Internet.

Forgery, fraud and theft

Private individuals and businesses must be protected from electronic forgery, fraud and theft. New provisions such as these update our laws, demonstrating that individuals and companies have an "online" identity that can be used by others in criminal or malicious activity. Fraud statutes must protect Internet consumers and businesses against crimes such as theft of trade secrets, credit card fraud, identity theft and forgery.

Cyberstalking

Current statutes did not provide adequate protection from cyberstalking, where physical contact between the victim and stalker may never occur. The new legislation includes the unique and technical aspect of cyberstalking and provides an effective tool for prosecution and prevention.

Computer use and disruption

When a company or an individual loses their access to the Internet, they can lose contact to their customers, business records, financial information, and other materials hindering their ability to work, retrieve data, and communicate. This section is designed to deter several forms of disruption which have not been covered by the current statute.

Child pornography

The section protects computer repair technicians and others who report child pornography to the police. It also adds the offense of "luring," to attack effectively the online solicitation or offering of a child with an intent of sexual exploitation. Individuals would be held criminally liable for any sexually explicit material knowingly transmitted to a school or minor.

The Computer Crimes Act of 2000 goes into effect July 18, 2000.

EMERGING ISSUES

Law enforcement and the public at large have raised several issues that Congress and the states will have to come to terms with in the near future. Two of the ones my office is working on are Privacy and the Theft of Intellectual Property.

Privacy

The public is becoming increasingly concerned over the collection and ownership of personal identifying information. The traditional American model is that organizations that gather information about individuals become the owners of that information, and can use it for their own purposes or even sell it to others. The phrase seen in hacker chat rooms currently is, "You have no privacy now—get over it."

On the other hand, for 25 years or more, many countries have had strong privacy protections including transborder data flow statutes prohibiting the transfer of personal data across national boundaries, and others laws forbidding the "secondary use" of personal data without permission of the individual. In fact, American corporations have just agreed to honor European Union privacy rules which are much more stringent than any they observe in this country, in connection with our own citizens' data.

We have made tremendous advances with the use of the Internet in numerous fields. But at the same time, the Internet poses a threat to individual privacy—and security—on a scale never imaginable in earlier times, when records pertaining to individuals were maintained by corporations and public agencies in separate files scattered across the business and government landscapes.

The time has come for a comprehensive assessment of our nation's business practices with regard to the collection and use of personal data. The national epidemic of Identity Theft crimes is proof that we also need to establish industry standards for maintaining the security and accuracy of information that is collected about individuals. I intend to work with Arizona business, consumer and privacy groups in the next legislative session to craft legislation that will offer our citizens reasonable assurance that they know what information is being collected about them, have an opportunity to correct inaccuracies, and have some say in what is done with their personal data. I believe that, working together, Arizona citizens and businesses can establish a reasonable framework for protecting individual privacy in a world where all records are online, all the time.

Theft of intellectual property

The Internet has also caused another revolution—the quick and rapid distribution of many perfect copies of the same original. Arizona's "Silicon Desert" is an important and fast-growing part of our economy, and the protection of our information resources is critical. Currently, the Federal copyright statute preempts the states from enforcing thefts of intellectual property such as software, video and music, yet the Federal agencies only have the resources to pursue a tiny fraction of the reported offenses. This situation robs our American businesses of billions of dollars a year, and allows the thieves to flourish.

As a former United States Attorney, I understand the limitations of resources among the Federal agencies. However, every year a number of business victims come to our office for help, but the Federal preemption of copyright theft leaves us powerless to help them. I know that industry would support a change in the copyright law to permit enforcement at the state level, and I urge Congress to amend the copyright laws to permit enforcement by both Federal and State agencies. A strong information economy requires strong protection for our information assets.

CONCLUSION—CURRENT CHALLENGES

The Arizona Attorney General's Office is charging ahead in partnership with various groups to address Arizona's state of emergency regarding cybercrime.

- *Law Enforcement*—we have created a three-tiered training program:

1. A two-day comprehensive evidence seizure and crime scene procedure class. This will be certified by AZ POST and taught by the Department of Public Safety, the Attorney General's Office and other agencies. The goal is to create regional expert teams, similar to the meth lab multi-agency teams, and certify 200 officers in the State.
2. Police officers training to teach various tools and programs for extracting computer evidence and creating a case ready for prosecution.
3. Detective training to teach the special skills necessary to perform investigations in cyberspace.

• *Communication Industry*—We are working with on-line providers to develop standardized policies and forms for legal procedures necessary to obtain computer evidence.

• *Business*—We are working with corporations to assist in raising awareness on computer security issues and using their expertise to help train law enforcement.

• *Schools*—We are working closely with schools and school districts to deal with the increasing problem of school online threats.

• *Public*—We are conducting townhalls throughout Arizona to educate the public at large particularly seniors and parents, to potential dangers on the Internet.

In addition to the work being done in Arizona, other states have also been active: California has established regional task forces; the Attorney General of Illinois has established a state level unit to investigate and prosecute computer crimes; and the Attorney General of South Carolina has, with the assistance of the Office of Juvenile Justice and Delinquency Programs in the U.S. Department of Justice, created a task force to investigate and prosecute child pornographers and pedophiles. In fact, Attorneys General from around the country have made cybercrime a high priority for the National Association of Attorneys General.

But like Arizona, states face two major obstacles in setting up units or task forces to address computer crimes: staff and equipment. Attorneys, investigators and prosecutors with computer skills are in high demand. Unable to hire and retain these skilled professionals at state salaries, states have turned to grooming these professionals within current ranks. Training, however, is expensive and not enough police and prosecutors are receiving it. Equipment to investigate these crimes is also expensive and must be constantly updated to keep pace with technology.

Participation of the states in protecting the nation's infrastructure by investigating and prosecuting computer crimes is critical. As in other areas of criminal law, the states will undoubtedly carry the bulk of the computer crime investigations and prosecutions and, in the area of juvenile prosecutions, the states will have the full burden of those cases. This burden is likely to be considerable because computers have become ubiquitous in almost every type of crime.

The efforts of Arizona and other states to address computer crimes must be nurtured by the Federal Government. The states need direct Federal funding to establish computer forensic laboratories.

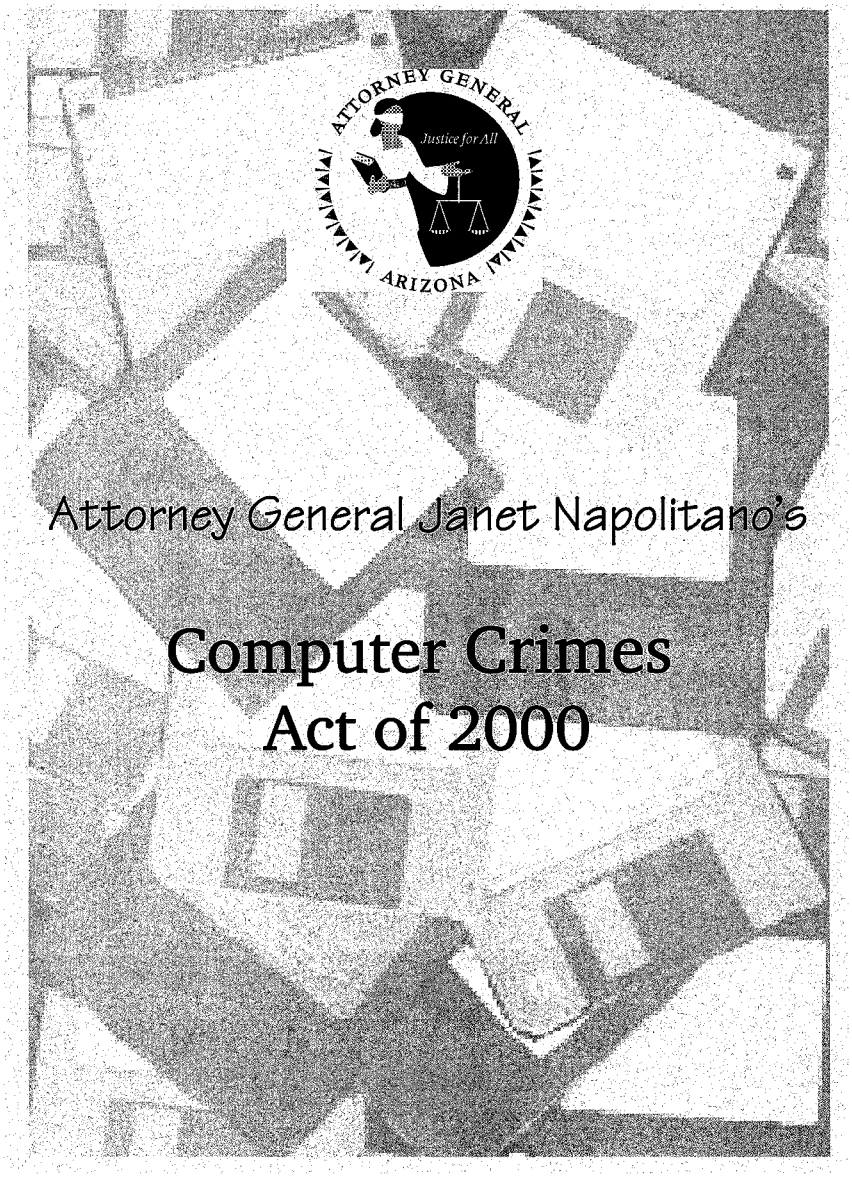
The development of a basic curriculum for prosecutors is underway. The means to execute the training and to provide ongoing technical assistance exists through the National Association of Attorneys General and the National District Attorneys Association. Unfortunately, we are missing the funding to implement the training and assistance. Approximately $1 million a year for 5 years would allow over 100 prosecutors to be trained each year.

To combat cybercrime, states need a program to provide seed money to assist with hiring knowledgeable staff and buying much needed equipment should be established on the Federal level. This program would need to provide a minimum of $500,000 per year per state for at least 3 years to allow the states to establish programs and begin funding them.

Updates to the law, such as Arizona's Computer Crimes Act 2000, is a powerful first step in the battle against cybercriminals. But resources, applied intelligently, would revolutionize law enforcement's ability to respond swiftly and effectively to cybercrime.

I look forward to working with this Subcommittee and other Federal entities to ensure that we have a coordinated Federal-State effort to combat cybercrime.

Once again, thank you for inviting me to present the perspective of the Arizona Attorney General's Office and I would be pleased to answer any questions from Subcommittee members.



Attorney General Janet Napolitano's

Computer Crimes Act of 2000

Attorney General Janet Napolitano's Computer Crimes Act of 2000

Table of Contents

- Letter from the Attorney General
- Summary
- Computer Crimes Act
- Attorney General's Website
- News Articles

Attorney General Janet Napolitano's Computer Crimes Act of 2000

Letter from the Attorney General

STATE OF ARIZONA

OFFICE OF THE ATTORNEY GENERAL

JANET NAPOLITANO
ATTORNEY GENERAL

1275 WEST WASHINGTON, PHOENIX, AZ. 85007-2926

MAIN PHONE: (602) 542-5025
FACSIMILE: (602) 542-4085

April, 2000

As Attorney General for the State of Arizona, my Office is dedicated to enforcing the law whenever and wherever it is broken. Fortunately, our communities have seen a marked decline in violent crime. Less encouraging is the rate of crimes committed using computers and other emerging technologies.

In fact, cybercrime has increased so exponentially that law enforcement has had a difficult time keeping up. The speed with which technology advances demands rapid and innovative solutions to complex problems. Arizona law was simply inadequate in dealing with the challenges presented by the hi-tech 21st century.

The Computer Crimes Act of 2000 was authored to address the deficiencies in existing law making it difficult to effectively prosecute criminals. With bipartisan support, the bill was passed by the Arizona legislature and becomes effective July 18, 2000.

Enclosed please find a summary of the Computer Crimes Act of 2000, the complete language of the bill and relevant Arizona news clippings describing some of the deficiencies the Act is intended to address as well as highlights of the process. I hope you find this information useful.

Sincerely,

Janet Napolitano
Attorney General
State of Arizona

Attorney General Janet Napolitano's Computer Crimes Act of 2000

Summary

The Computer Crimes Act of 2000

There are six parts to this legislation:

- ***Cyberterrorism***

We must use every means available to crack down on attacks on our high-tech infrastructure. This section raises judicial penalties for disrupting operations of utilities, emergency services, medical institutions, traffic control, etc.

- ***Cybertools for Law Enforcement***

The cybertools strengthens law enforcement's ability to preserve electronic evidence and to rapidly trace criminal activity on the Internet.

- ***Forgery, Fraud and Theft***

Private individuals and businesses must be protected from electronic forgery, fraud and theft. This updates our laws, acknowledging that individuals and companies have an "online" identity that can be used by others in criminal or malicious activity. Fraud statutes must protect Internet consumers and businesses against theft of trade secrets, credit card fraud, identity theft and forgery.

- ***Cyberstalking***

Current statutes did not provide adequate protection from cyberstalking, where physical contact between the victim and stalker may never even take place. This section includes the unique and technical aspect of cyberstalking and provides an effective tool for prosecution and prevention.

- ***Computer Use and Disruption***

When a company or an individual loses their access to the Internet, they can lose access to their customers, business records, financial information and other materials that hinder their ability to work, retrieve data and communicate. This section is designed to deter several forms of disruption which have not been covered by the current statute.

- ***Child Pornography***

The section protects computer repair technicians or others who report child pornography to the police from civil liability. It also adds the offense of "luring," to attack effectively the online solicitation or offering of a child with an intent of sexual exploitation. Individuals would be held criminally liable for any sexually explicit material knowingly transmitted to a school or minor.

Attorney General Janet Napolitano's Computer Crimes Act of 2000

Computer Crimes Act

House Engrossed

FILED

Betsey Bayless
Secretary of State

State of Arizona
House of Representatives
Forty-fourth Legislature
Second Regular Session
2000

CHAPTER 189

HOUSE BILL 2428

AN ACT

AMENDING SECTIONS 12-731, 12-741, 13-1801, 13-1802, 13-2001, 13-2002, 13-2003 AND 13-2301, ARIZONA REVISED STATUTES; TRANSFERRING AND RENUMBERING SECTION 13-2708, ARIZONA REVISED STATUTES, FOR PLACEMENT IN TITLE 13, CHAPTER 20, ARIZONA REVISED STATUTES, AS SECTION 13-2008; AMENDING SECTION 13-2008, ARIZONA REVISED STATUTES, AS TRANSFERRED AND RENUMBERED BY THIS ACT; AMENDING SECTION 13-2316, ARIZONA REVISED STATUTES; AMENDING TITLE 13, CHAPTER 23, ARIZONA REVISED STATUTES, BY ADDING SECTIONS 13-2316.01 AND 13-2316.02; REPEALING SECTIONS 13-2912, 13-2913 AND 13-2914, ARIZONA REVISED STATUTES; RENUMBERING SECTION 13-3004, ARIZONA REVISED STATUTES, AS SECTION 13-3001; RENUMBERING SECTION 13-3001, ARIZONA REVISED STATUTES, AS SECTION 13-3004; AMENDING SECTION 13-3001, ARIZONA REVISED STATUTES, AS RENUMBERED BY THIS ACT; AMENDING SECTIONS 13-3008, 13-3010, 13-3011, 13-3012, 13-3013 AND 13-3016, ARIZONA REVISED STATUTES; RENUMBERING SECTION 13-3018, ARIZONA REVISED STATUTES, AS SECTION 13-3019; AMENDING TITLE 13, CHAPTER 30, ARIZONA REVISED STATUTES, BY ADDING A NEW SECTION 13-3018; AMENDING SECTION 13-3019, AS RENUMBERED BY THIS ACT; AMENDING SECTIONS 13-3417, 13-3506, 13-3551 AND 13-3553, ARIZONA REVISED STATUTES; REPEALING SECTION 13-3508, ARIZONA REVISED STATUTES; RENUMBERING SECTIONS 13-3554, 13-3555 AND 13-3556, ARIZONA REVISED STATUTES, AS SECTIONS 13-3555, 13-3556 AND 13-3558, RESPECTIVELY; AMENDING TITLE 13, CHAPTER 35.1, ARIZONA REVISED STATUTES, BY ADDING A NEW SECTION 13-3554; AMENDING TITLE 13, CHAPTER 35.1, ARIZONA REVISED STATUTES, BY ADDING SECTIONS 13-3557 AND 13-3559; AMENDING SECTIONS 13-3707, 13-4801, 21-422, 31-281 AND 44-405, ARIZONA REVISED STATUTES; RELATING TO TECHNOLOGY CRIMES.

(TEXT OF BILL BEGINS ON NEXT PAGE)

Be it enacted by the Legislature of the State of Arizona:

Section 1. Section 12-731, Arizona Revised Statutes, is amended to read:

12-731. Recovery of civil damages

A. Except as provided in ~~this section and section 13-3012~~ TITLE 13, CHAPTER 30, any person whose wire, oral or electronic communication is intentionally intercepted, disclosed or used in violation of ~~this chapter~~ TITLE 13, CHAPTER 30 may ~~in~~ BRING a civil action TO recover from the person or entity ~~which~~ THAT engaged in ~~that~~ THE violation the following:

1. Such preliminary and other equitable or declaratory relief as may be appropriate.

2. Damages in an amount ~~which~~ THAT is the greater of EITHER:

(a) The sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation.

(b) Statutory damages of one hundred dollars a day for each day of the violation.

(c) Statutory damages of ten thousand dollars.

3. Punitive damages in appropriate cases.

4. Reasonable attorney fees and other reasonable costs of litigation.

B. A civil action under this section may not be commenced later than one year after the date upon which the ~~claimant~~ PLAINTIFF first has a reasonable opportunity to discover the violation.

Sec. 2. Section 12-741, Arizona Revised Statutes, is amended to read:

12-741. Definitions

In this article, unless the context otherwise requires:

1. "Buyer" means a person who leases, licenses or purchases any product, equipment or service.

2. "Computer" has the same meaning prescribed in section 13-2301, subsection E.

~~3. "Computer network" has the same meaning prescribed in section 13-2301, subsection E.~~

~~4.~~ 3. "Computer program" has the same meaning prescribed in section 13-2301, subsection E.

~~5.~~ 4. "Computer software" has the same meaning prescribed in section 13-2301, subsection E.

~~6.~~ 5. "Computer system" has the same meaning prescribed in section 13-2301, subsection E.

~~7.~~ 6. "Equipment" means any item that contains a product and that is used to produce or deliver a product or service.

7. "NETWORK" HAS THE SAME MEANING PRESCRIBED IN SECTION 13-2301, SUBSECTION E.

8. "Product" means any item that is:

(a) Directly or indirectly manufactured, created or delivered by or that operates through the use of embedded chips or through the manipulation of electronic or magnetic impulses, including any computer, ~~computer~~ network,

computer program, computer software or computer system or any constituent component, any item that contains an integrated circuit or any other electronics component.

(b) Directly or indirectly manufactured, created or delivered by or that operates through the use of an integrated circuit or electronic component.

9. "Remedial measures" means an action that is taken to improve the efficacy of any product, equipment or service in order to lessen the likelihood or consequences of a year 2000 date failure. These actions may include:

(a) Modifications to the product, equipment or service.

(b) Changes in quality assurance procedures or policies.

(c) Modifications that are made to the design or method of manufacturing, to manufacturing equipment or to the testing of the product, equipment or service.

(d) Changes in or additions to training programs or safety education programs.

(e) Personnel or human resources measures that are related to the product, equipment or service.

(f) The use or modification of warnings or notices or changes to owner manuals and related materials.

(g) The recall of products.

(h) The creation of a plan or instructions to be implemented in the event of or to avoid a year 2000 date failure.

(i) Alternative services that are offered in connection with a service to provide the buyer with the intended result of the service.

10. "Service" means any effort, function, labor, delivery, processing or time that directly or indirectly involves the use of a product.

11. "Year 2000 compliance analysis or review" means any evaluation, investigation, inquiry, review or other means by which a person seeks to compute, determine, estimate, evaluate, predict or report the performance of any product, equipment or service and that may be conducted by employees or agents of the person, by a year 2000 consultant or by a government agency or instrumentality.

12. "Year 2000 date failure" means either:

(a) The present or future failure or inability of a product or any product or equipment that uses a product to accurately accept, compute, compare, distinguish, generate, interpret, produce, recognize, sequence or otherwise process, store or display correctly date and time data in, from, into and between the years 1999 and 2000 and subsequent years, the twentieth and twenty-first centuries and leap year computations.

(b) The present or future failure or inability of a service that uses a product or equipment that fails or is not able to accurately accept, compute, compare, distinguish, generate, interpret, produce, recognize, sequence or otherwise process, store or display date and time data in, from,

into and between the years 1999 and 2000 and subsequent years, the twentieth and twenty-first centuries and leap year computations.

~~13. "Year 2000 date statement" means a statement that is material to a transaction made about a product that is manufactured or sold or about a service that is provided or sold regarding whether the product, equipment or service will result in a year 2000 date failure.~~

Sec. 3. Section 13-1801, Arizona Revised Statutes, is amended to read:

13-1801. Definitions

A. In this chapter, unless the context otherwise requires:

1. "Check" means any check, draft or other negotiable or nonnegotiable instrument of any kind.

2. "Control" or "exercise control" means to act so as to exclude others from using their property except on the defendant's own terms.

3. "Credit" means an express agreement with the drawee for the payment of a check.

4. "Deprive" means to withhold the property interest of another either permanently or for so long a time period that a substantial portion of its economic value or usefulness or enjoyment is lost, ~~or~~ to withhold it with the intent to restore it only upon payment of ANY reward or other compensation or to transfer or dispose of it so that it is unlikely to be recovered.

5. "Draw" means making, drawing, uttering, preparing, writing or delivering a check.

6. "Funds" ~~mean~~ MEANS money or credit.

7. "Issue" means to deliver or cause to be delivered a check to a person who thereby acquires a right against the drawer with respect to the check. A person who draws a check with THE intent that it be so delivered is deemed to have issued it if the delivery occurs.

8. "Material misrepresentation" means A pretense, promise, representation or statement of present, past or future fact ~~which~~ THAT is fraudulent and ~~which~~ THAT, when used or communicated, is instrumental in causing the wrongful control or transfer of property or services. The pretense may be verbal or it may be a physical act.

9. "Means of transportation" means any vehicle.

10. "Obtain" means to bring about or TO receive the transfer of any interest in property, whether to a defendant or to another, or to secure THE performance of a service OR THE POSSESSION OF A TRADE SECRET.

11. "Pass" means, for a payee, holder or bearer of a check ~~which~~ THAT previously has been or purports to have been drawn and issued by another, to deliver a check, for a purpose other than collection, to a third person who by delivery acquires a right with respect to the check.

12. "PROPERTY" MEANS ANY THING OF VALUE, TANGIBLE OR INTANGIBLE, INCLUDING TRADE SECRETS.

~~12.~~ 13. "Property of another" means property in which any person other than the defendant has an interest ON which the defendant is not privileged to infringe, including property in which the defendant also has an interest,

notwithstanding the fact that the other person might be precluded from civil recovery because the property was used in an unlawful transaction or was subject to forfeiture as contraband. Property in possession of the defendant is not deemed property of another person who has only a security interest in ~~such~~ THE property, even if legal title is in the creditor pursuant to a security agreement.

~~13.~~ 14. "Services" includes labor, professional ~~service~~ SERVICES, transportation, cable television, ~~telephone~~ COMPUTER OR COMMUNICATION SERVICES, gas or electricity services, accommodation in hotels, restaurants~~,~~ OR leased premises or elsewhere, admission to exhibitions and use of vehicles or other movable property.

~~14.~~ 15. "Value" means the fair market value of the property or services at the time of the theft. Written instruments ~~which~~ THAT do not have a readily ascertained market value have as their value either the face amount of indebtedness less the portion satisfied or the amount of economic loss involved in deprivation of the instrument, whichever is greater. When property has AN undeterminable value THE TRIER OF FACT SHALL DETERMINE its value ~~shall be determined by the trier of fact~~ and, in reaching its decision, MAY CONSIDER all relevant evidence, ~~may be considered~~ including evidence of ~~such~~ THE property's value to its owner.

B. IN DETERMINING THE CLASSIFICATION OF THE OFFENSE, THE STATE MAY AGGREGATE IN THE INDICTMENT OR INFORMATION amounts taken in thefts committed pursuant to one scheme or course of conduct, whether THE AMOUNTS WERE TAKEN from one or several persons~~, may be aggregated in the indictment or information at the discretion of the state in determining the classification of the offense~~.

Sec. 4. Section 13-1802, Arizona Revised Statutes, is amended to read:

13-1802. Theft; classification

A. A person commits theft if, without lawful authority, the person knowingly:

1. Controls property of another with the intent to deprive the other person of such property; or

2. Converts for an unauthorized term or use services or property of another entrusted to the defendant or placed in the defendant's possession for a limited, authorized term or use; or

3. Obtains ~~property or~~ services OR PROPERTY of another by means of any material misrepresentation with intent to deprive the other person of such property or services; or

4. Comes into control of lost, mislaid or misdelivered property of another under circumstances providing means of inquiry as to the true owner and appropriates such property to the person's own or another's use without reasonable efforts to notify the true owner; or

5. Controls property of another knowing or having reason to know that the property was stolen; or

6. Obtains services known to the defendant to be available only for compensation without paying or an agreement to pay ~~such~~ THE compensation or diverts another's services to the person's own or another's benefit without authority to do so.

B. A person commits theft if the person knowingly takes control, title, use or management of an incapacitated or vulnerable adult's assets or property through intimidation or deception, as defined in section 46-456, while acting in a position of trust and confidence and with the intent to deprive the incapacitated or vulnerable adult of the asset or property.

C. The inferences set forth in section 13-2305 ~~shall~~ apply to any prosecution under ~~the provisions of~~ subsection A, paragraph 5 of this section.

D. AT THE CONCLUSION OF ANY GRAND JURY PROCEEDING, HEARING OR TRIAL, THE COURT SHALL PRESERVE ANY TRADE SECRET THAT IS ADMITTED IN EVIDENCE OR ANY PORTION OF A TRANSCRIPT THAT CONTAINS INFORMATION RELATING TO THE TRADE SECRET PURSUANT TO SECTION 44-405.

~~D.~~ E. Theft of property or services with a value of twenty-five thousand dollars or more is a class 2 felony. Theft of property or services with a value of three thousand dollars or more but less than twenty-five thousand dollars is a class 3 felony. Theft of property or services with a value of two thousand dollars or more but less than three thousand dollars is a class 4 felony. Theft of property or services with a value of one thousand dollars or more but less than two thousand dollars is a class 5 felony. Theft of property or services with a value of two hundred fifty dollars or more but less than one thousand dollars is a class 6 felony. Theft of any property or services valued at less than two hundred fifty dollars is a class 1 misdemeanor, unless such property is taken from the person of another or is a firearm, in which case the theft is a class 6 felony.

~~E.~~ F. A person who is convicted of a violation of subsection A, paragraph 1 or 3 of this section that involved property with a value of one hundred thousand dollars or more is not eligible for suspension of sentence, probation, pardon or release from confinement on any basis except pursuant to section 31-233, subsection A or B until the sentence imposed by the court has been served, the person is eligible for release pursuant to section 41-1604.07 or the sentence is commuted.

Sec. 5. Section 13-2001, Arizona Revised Statutes, is amended to read:

13-2001. Definitions

In this chapter, unless the context otherwise requires:

1. "ACCESS DEVICE" MEANS ANY CARD, TOKEN, CODE, ACCOUNT NUMBER, ELECTRONIC SERIAL NUMBER, MOBILE OR PERSONAL IDENTIFICATION NUMBER, PASSWORD, ENCRYPTION KEY, BIOMETRIC IDENTIFIER OR OTHER MEANS OF ACCOUNT ACCESS, INCLUDING A CANCELED OR REVOKED ACCESS DEVICE, THAT CAN BE USED ALONE OR IN CONJUNCTION WITH ANOTHER ACCESS DEVICE TO OBTAIN MONEY, GOODS, SERVICES,

COMPUTER OR NETWORK ACCESS OR ANY OTHER THING OF VALUE OR THAT CAN BE USED TO INITIATE A TRANSFER OF ANY THING OF VALUE.

~~1.~~ 2. "Coin machine" means a coin box, turnstile, vending machine or other mechanical, electrical~~,~~ or electronic device or receptacle THAT IS designed to receive a coin or bill of a certain denomination or a token made for such purpose~~,~~ and THAT, in return for the insertion or deposit ~~thereof~~ OF THE COIN, BILL OR TOKEN, automatically ~~to offer, provide, assist~~ OFFERS, PROVIDES, ASSISTS in providing or ~~permit~~ PERMITS the acquisition or use of some property or service.

~~2.~~ 3. "Complete written instrument" means a written instrument ~~which~~ THAT purports to be genuine and fully drawn with respect to every essential feature ~~thereof~~.

~~6.~~ 4. "~~To~~ Falsely ~~alter~~ ALTERS a written instrument" means to change A COMPLETE OR INCOMPLETE WRITTEN INSTRUMENT, without the permission of anyone entitled to grant it, ~~a written instrument, whether complete or incomplete,~~ by means of erasure, obliteration, deletion, insertion of new matter~~,~~ OR transposition of matter or in any other manner, so that the altered instrument falsely appears or purports to be in all respects an authentic creation of its ostensible maker or authorized by him.

~~7.~~ 5. "~~To~~ Falsely ~~complete~~ COMPLETES a written instrument" means to transform an incomplete written instrument into a complete one by adding, inserting or changing matter without the permission of anyone entitled to grant it, so that the complete written instrument falsely appears or purports to be in all respects an authentic creation of its ostensible maker or authorized by him.

~~8.~~ 6. "~~To~~ Falsely ~~make~~ MAKES a written instrument" means to make or draw a complete or incomplete written instrument ~~which~~ THAT purports to be an authentic creation of its ostensible maker but ~~which~~ THAT is not either because the ostensible maker is fictitious, or because, if real, ~~he~~ THE OSTENSIBLE MAKER did not authorize the making or drawing of ~~such~~ THE written instrument.

~~3.~~ 7. "Forged instrument" means a written instrument ~~which~~ THAT has been falsely made, completed or altered.

~~4.~~ 8. "Incomplete written instrument" means a written instrument ~~which~~ THAT contains some matter by way of content or authentication but ~~which~~ THAT requires additional matter to render it a complete written instrument.

9. "PERSONAL IDENTIFYING INFORMATION" MEANS A NAME, ELECTRONIC IDENTIFIER OR SCREEN NAME, BIOMETRIC IDENTIFIER, DRIVER LICENSE NUMBER, ACCESS DEVICE, RESIDENCE OR MAILING ADDRESS, TELEPHONE NUMBER, EMPLOYER, STUDENT OR MILITARY IDENTIFICATION NUMBER, SOCIAL SECURITY NUMBER OR BIRTH DATE.

~~5.~~ 10. "Slug" means an object, article or device ~~which~~ THAT by virtue of its size, ITS shape or any other quality is capable of being inserted, deposited or otherwise used in a coin machine as a fraudulent substitute for a genuine token, lawful coin~~,~~ or bill of the United States.

~~9.~~ 11. "Written instrument" means EITHER:

(a) Any paper, document or other instrument ~~containing~~ THAT CONTAINS written or printed matter or its equivalent~~; or~~.

(b) Any token, stamp, seal, badge, trademark, GRAPHICAL IMAGE, ACCESS DEVICE or other evidence or symbol of value, right, privilege or identification.

Sec. 6. Section 13-2002, Arizona Revised Statutes, is amended to read:

13-2002. Forgery; classification

A. A person commits forgery if, with intent to defraud, ~~such~~ THE person:

1. Falsely makes, completes or alters a written instrument; or

2. Knowingly possesses a forged instrument; or

3. Offers or presents, whether accepted or not, a forged instrument or one ~~which~~ THAT contains false information.

B. THE POSSESSION OF FIVE OR MORE FORGED INSTRUMENTS MAY GIVE RISE TO AN INFERENCE THAT THE INSTRUMENTS ARE POSSESSED WITH AN INTENT TO DEFRAUD.

~~B.~~ C. Forgery is a class 4 felony.

Sec. 7. Section 13-2003, Arizona Revised Statutes, is amended to read:

13-2003. Criminal possession of a forgery device; classification

A. A person commits criminal possession of a forgery device if ~~such~~ THE person EITHER:

1. Makes or possesses with knowledge of its character any plate, die, or other device, apparatus, equipment, SOFTWARE, ACCESS DEVICE or article specifically designed or adapted for use in forging written instruments~~; or~~.

2. Makes or possesses any device, apparatus, equipment, SOFTWARE, ACCESS DEVICE or article adaptable for use in forging written instruments with intent to use it or to aid or permit another to use it for purposes of forgery.

B. SUBSECTION A, PARAGRAPH 1 DOES NOT APPLY TO PEACE OFFICERS OR PROSECUTORS IN THE PERFORMANCE OF THEIR DUTIES.

~~B.~~ C. ~~Criminal possession of a forgery device in~~ A VIOLATION OF subsection A, paragraph 1 is a class 6 felony. ~~Criminal possession of a forgery device in~~ A VIOLATION OF subsection A, paragraph 2 is a class 5 felony.

Sec. 8. Section 13-2708, Arizona Revised Statutes, is transferred and renumbered for placement in title 13, chapter 20, Arizona Revised Statutes, as section 13-2008 and, as so renumbered, is amended to read:

13-2008. Taking identity of another person; classification

A. A person commits taking the identity of another person if the person knowingly takes ~~the name, birth date or social security number~~ OR USES ANY PERSONAL IDENTIFYING INFORMATION of another person, without the consent of that other person, with the intent to obtain or use the other person's identity for any unlawful purpose or to cause loss to a person.

B. A PEACE OFFICER IN ANY JURISDICTION IN WHICH AN ELEMENT OF THE OFFENSE IS COMMITTED OR A RESULT OF THE OFFENSE OCCURS MAY TAKE A REPORT.

C. IF A DEFENDANT IS ALLEGED TO HAVE COMMITTED MULTIPLE VIOLATIONS OF THIS SECTION WITHIN THE SAME COUNTY, THE PROSECUTOR MAY FILE A COMPLAINT CHARGING ALL OF THE VIOLATIONS AND ANY RELATED CHARGES UNDER OTHER SECTIONS THAT HAVE NOT BEEN PREVIOUSLY FILED IN THE JUSTICE OF THE PEACE PRECINCT IN WHICH THE GREATEST NUMBER OF VIOLATIONS ARE ALLEGED TO HAVE OCCURRED.

~~B.~~ D. Taking the identity of another person is a class ~~5~~ 4 felony.

E. FOR THE PURPOSES OF THIS SECTION, "VICTIM" INCLUDES A PERSON WHOSE PERSONAL IDENTIFYING INFORMATION IS TAKEN OR USED WITHOUT CONSENT, WHETHER OR NOT THE VICTIM ACTUALLY SUFFERS ANY ECONOMIC LOSS AS A RESULT OF THE OFFENSE.

Sec. 9. Section 13-2301, Arizona Revised Statutes, is amended to read:

13-2301. Definitions

A. For the purposes of sections 13-2302 ~~through~~, 13-2303 AND 13-2304:

~~6.~~ 1. "~~To~~ Collect an extension of credit" means to induce in any way any person to make repayment ~~thereof~~ OF THAT EXTENSION.

~~1.~~ 2. "Creditor" means any person making ~~such~~ an extension of credit or any person claiming by, under~~,~~ or through any person making ~~such~~ an extension of credit.

~~2.~~ 3. "Debtor" means any person to whom ~~such~~ an extension of credit is made or any person who guarantees the repayment of an extension of credit, or in any manner undertakes to indemnify the creditor against loss resulting from the failure of any person to whom an extension is made to repay the ~~same~~ EXTENSION.

~~7.~~ 4. "~~To~~ Extend credit" means to make or renew any loan or to enter into any agreement, tacit or express, whereby the repayment or satisfaction of any debt or claim, whether acknowledged or disputed, valid or invalid, and however arising, may or shall be deferred.

~~5.~~ 5. "Extortionate extension of credit" means any extension of credit with respect to which it is the understanding of the creditor and the debtor at the time ~~such~~ THE extension is made that delay in making repayment or failure to make repayment could result in the use of violence or other criminal means to cause harm to the person or the reputation or property of any person.

~~4.~~ 6. "Extortionate means" means the use, or an express or implicit threat of use, of violence or other criminal means to cause harm to the person or the reputation or property of any person.

~~5.~~ 7. "Repayment of any extension of credit" means the repayment, satisfaction or discharge in whole or in part of any debt or claim, acknowledged or disputed, valid or invalid, resulting from or in connection with that extension of credit.

B. For the purposes of ~~sections~~ SECTION 13-2305 ~~through~~, 13-2306 OR 13-2307:

1. "Dealer in property" means a person who buys and sells property as a business.

2. "Stolen property" means property OF ANOTHER AS DEFINED IN SECTION 13-1801 that has been the subject of any unlawful taking.

3. "Traffic" means to sell, transfer, distribute, dispense or otherwise dispose of stolen property to another person, or to buy, receive, possess or obtain control of stolen property, with THE intent to sell, transfer, distribute, dispense or otherwise dispose of THE PROPERTY to another person.

C. For the purposes of this chapter:

1. "Combination" means persons who collaborate in carrying on or furthering the activities or purposes of a criminal syndicate even though such persons may not know each other's identity, membership in the combination changes from time to time or one or more members may stand in a wholesaler-retailer or other arm's length relationship with others as to activities or dealings between or among themselves in an illicit operation.

2. "Criminal syndicate" means any combination of persons or enterprises engaging, or having the purpose of engaging, on a continuing basis in conduct ~~which~~ THAT violates any one or more provisions of any felony statute of this state.

D. For the purposes of sections 13-2312 through 13-2315, unless the context otherwise requires:

1. "Control", in relation to an enterprise, means the possession of sufficient means to permit substantial direction over the affairs of an enterprise and, in relation to property, means to acquire or possess.

2. "Enterprise" means any corporation, partnership, association, labor union~~,~~ or other legal entity or any group of persons associated in fact although not a legal entity.

3. "Financial institution" means any business under the jurisdiction of the state banking department or a banking or securities regulatory agency of the United States or a business under the jurisdiction of the securities division of the corporation commission, the state real estate department or the department of insurance.

4. "Racketeering" means any act, including any preparatory or completed offense, ~~which~~ THAT is committed for financial gain, ~~which~~ THAT is chargeable or indictable under the laws of the state in which the act occurred and, if the act occurred in a state other than this state, ~~which~~ THAT would be chargeable or indictable under the laws of this state ~~had~~ IF the act HAD occurred in this state and ~~which~~ THAT would be punishable by imprisonment for more than one year, regardless of whether such act is charged or indicted, involving:

(a) Homicide.

(b) Robbery.

(c) Kidnapping.

(d) Forgery.

(e) Theft.
(f) Bribery.
(g) Gambling.
(h) Usury.
(i) Extortion.
(j) Extortionate extensions of credit.
(k) Prohibited drugs, marijuana or other prohibited chemicals or substances.
(l) Trafficking in explosives, weapons or stolen property.
(m) Participating in a criminal syndicate.
(n) Obstructing or hindering criminal investigations or prosecutions.
(o) Asserting false claims including, but not limited to, false claims asserted through fraud or arson.
(p) Intentional or reckless false statements or publications concerning land for sale or lease or sale of subdivided lands or sale and mortgaging of unsubdivided lands.
(q) Resale of realty with intent to defraud.
(r) Intentional or reckless fraud in the purchase or sale of securities.
(s) Intentional or reckless sale of unregistered securities or real property securities.
(t) A scheme or artifice to defraud.
(u) Obscenity.
~~(v) Child pornography.~~
(v) SEXUAL EXPLOITATION OF CHILDREN.
(w) Prostitution.
(x) Restraint of trade or commerce in violation of section 34-252.
(y) Terrorism.
(z) Money laundering.
(aa) Obscene or indecent telephone communications to minors for commercial purposes.
(bb) Counterfeiting marks as proscribed in section 44-1453.

5. "Records" means any book, paper, writing, ~~record,~~ computer program, ~~or other material~~ DATA, IMAGE OR INFORMATION THAT IS COLLECTED, RECORDED, PRESERVED OR MAINTAINED IN ANY FORM OF STORAGE MEDIUM.

6. "~~To~~ Remedy racketeering" means to enter a civil judgment pursuant to this chapter or chapter 39 of this title against property or a person who is subject to liability, including liability for injury to the state that is caused by racketeering or by actions in concert with racketeering.

E. For the purposes of ~~section~~ SECTIONS 13-2316, 13-2316.01 AND 13-2316.02:

1. "Access" means to ~~approach,~~ instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or ~~computer~~ network.

2. "ACCESS DEVICE" MEANS ANY CARD, TOKEN, CODE, ACCOUNT NUMBER, ELECTRONIC SERIAL NUMBER, MOBILE OR PERSONAL IDENTIFICATION NUMBER, PASSWORD, ENCRYPTION KEY, BIOMETRIC IDENTIFIER OR OTHER MEANS OF ACCOUNT ACCESS, INCLUDING A CANCELED OR REVOKED ACCESS DEVICE, THAT CAN BE USED ALONE OR IN CONJUNCTION WITH ANOTHER ACCESS DEVICE TO OBTAIN MONEY, GOODS, SERVICES, COMPUTER OR NETWORK ACCESS OR ANY OTHER THING OF VALUE OR THAT CAN BE USED TO INITIATE A TRANSFER OF ANY THING OF VALUE.

~~2.~~ 3. "Computer" means an electronic device ~~which~~ THAT performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities ~~which~~ THAT are connected or related to such a device in a system or network.

~~3. "Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of two or more interconnected computers.~~

4. "COMPUTER CONTAMINANT" MEANS ANY SET OF COMPUTER INSTRUCTIONS THAT IS DESIGNED TO MODIFY, DAMAGE, DESTROY, RECORD OR TRANSMIT INFORMATION WITHIN A COMPUTER, COMPUTER SYSTEM OR NETWORK WITHOUT THE INTENT OR PERMISSION OF THE OWNER OF THE INFORMATION, COMPUTER SYSTEM OR NETWORK. COMPUTER CONTAMINANT INCLUDES A GROUP OF COMPUTER INSTRUCTIONS, SUCH AS VIRUSES OR WORMS, THAT IS SELF-REPLICATING OR SELF-PROPAGATING AND THAT IS DESIGNED TO CONTAMINATE OTHER COMPUTER PROGRAMS OR COMPUTER DATA, TO CONSUME COMPUTER RESOURCES, TO MODIFY, DESTROY, RECORD OR TRANSMIT DATA OR IN SOME OTHER FASHION TO USURP THE NORMAL OPERATION OF THE COMPUTER, COMPUTER SYSTEM OR NETWORK.

~~4.~~ 5. "Computer program" means a series of instructions or statements, in a form acceptable to a computer, ~~which~~ THAT permits the functioning of a computer system in a manner designed to provide appropriate products from ~~such~~ THE computer system.

~~5.~~ 6. "Computer software" means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

~~6.~~ 7. "Computer system" means a set of related, connected or unconnected computer equipment, devices and software, INCLUDING STORAGE, MEDIA AND PERIPHERAL DEVICES.

8. "CRITICAL INFRASTRUCTURE RESOURCE" MEANS ANY COMPUTER OR COMMUNICATIONS SYSTEM OR NETWORK THAT IS INVOLVED IN PROVIDING SERVICES NECESSARY TO ENSURE OR PROTECT THE PUBLIC HEALTH, SAFETY OR WELFARE, INCLUDING SERVICES THAT ARE PROVIDED BY ANY OF THE FOLLOWING:

(a) MEDICAL PERSONNEL AND INSTITUTIONS.

(b) EMERGENCY SERVICES AGENCIES.

(c) PUBLIC AND PRIVATE UTILITIES, INCLUDING WATER, POWER, COMMUNICATIONS AND TRANSPORTATION SERVICES.

(d) FIRE DEPARTMENTS, DISTRICTS OR VOLUNTEER ORGANIZATIONS.
(e) LAW ENFORCEMENT AGENCIES.
(f) FINANCIAL INSTITUTIONS.
(g) PUBLIC EDUCATIONAL INSTITUTIONS.
(h) GOVERNMENT AGENCIES.

9. "FALSE OR FRAUDULENT PRETENSE" MEANS THE UNAUTHORIZED USE OF AN ACCESS DEVICE OR THE USE OF AN ACCESS DEVICE TO EXCEED AUTHORIZED ACCESS.

~~7.~~ 10. "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card or marketable security or any other written instrument~~,~~ as defined ~~by~~ IN section 13-2001~~, paragraph 7, which~~ THAT is transferable for value.

11. "NETWORK" INCLUDES A COMPLEX OF INTERCONNECTED COMPUTER OR COMMUNICATION SYSTEMS OF ANY TYPE.

~~8.~~ 12. "Property" means financial instruments, information, including electronically produced data, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible.

13. "PROPRIETARY OR CONFIDENTIAL COMPUTER SECURITY INFORMATION" MEANS INFORMATION ABOUT A PARTICULAR COMPUTER, COMPUTER SYSTEM OR NETWORK THAT RELATES TO ITS ACCESS DEVICES, SECURITY PRACTICES, METHODS AND SYSTEMS, ARCHITECTURE, COMMUNICATIONS FACILITIES, ENCRYPTION METHODS AND SYSTEM VULNERABILITIES AND THAT IS NOT MADE AVAILABLE TO THE PUBLIC BY ITS OWNER OR OPERATOR.

~~9.~~ 14. "Services" includes computer time, data processing, ~~and~~ storage functions AND ALL TYPES OF COMMUNICATION FUNCTIONS.

Sec. 10. Section 13-2316, Arizona Revised Statutes, is amended to read:

13-2316. Computer tampering; venue; forfeiture; classification

A. A person WHO ACTS WITHOUT AUTHORITY OR WHO EXCEEDS AUTHORIZATION OF USE commits computer ~~fraud in the first degree~~ TAMPERING BY:

1. Accessing, altering, damaging or destroying ~~without authorization or exceeding authorization of use of~~ any computer, computer system~~, computer~~ OR network, or any part of ~~such~~ A computer, COMPUTER system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or TO control property or services by means of false or fraudulent pretenses, representations or promises.

2. KNOWINGLY ALTERING, DAMAGING, DELETING OR DESTROYING COMPUTER PROGRAMS OR DATA.

3. KNOWINGLY INTRODUCING A COMPUTER CONTAMINANT INTO ANY COMPUTER, COMPUTER SYSTEM OR NETWORK.

4. RECKLESSLY DISRUPTING OR CAUSING THE DISRUPTION OF COMPUTER, COMPUTER SYSTEM OR NETWORK SERVICES OR DENYING OR CAUSING THE DENIAL OF COMPUTER OR NETWORK SERVICES TO ANY AUTHORIZED USER OF A COMPUTER, COMPUTER SYSTEM OR NETWORK.

5. RECKLESSLY USING A COMPUTER, COMPUTER SYSTEM OR NETWORK TO ENGAGE IN A SCHEME OR COURSE OF CONDUCT THAT IS DIRECTED AT ANOTHER PERSON AND THAT SERIOUSLY ALARMS, TORMENTS, THREATENS OR TERRORIZES THE PERSON. FOR THE PURPOSES OF THIS PARAGRAPH, THE CONDUCT MUST BOTH:

(a) CAUSE A REASONABLE PERSON TO SUFFER SUBSTANTIAL EMOTIONAL DISTRESS.

(b) SERVE NO LEGITIMATE PURPOSE.

6. PREVENTING A COMPUTER USER FROM EXITING A SITE, COMPUTER SYSTEM OR NETWORK-CONNECTED LOCATION IN ORDER TO COMPEL THE USER'S COMPUTER TO CONTINUE COMMUNICATING WITH, CONNECTING TO OR DISPLAYING THE CONTENT OF THE SERVICE, SITE OR SYSTEM.

7. KNOWINGLY OBTAINING ANY INFORMATION THAT IS REQUIRED BY LAW TO BE KEPT CONFIDENTIAL OR ANY RECORDS THAT ARE NOT PUBLIC RECORDS BY ACCESSING ANY COMPUTER, COMPUTER SYSTEM OR NETWORK THAT IS OPERATED BY THIS STATE, A POLITICAL SUBDIVISION OF THIS STATE OR A MEDICAL INSTITUTION.

~~6.~~ 8. ~~A person commits computer fraud in the second degree by intentionally and without authorization, or by exceeding authorization~~ KNOWINGLY accessing~~, altering, damaging or destroying~~ any computer, computer system or ~~computer~~ network or any computer software, program or data THAT IS contained in ~~such~~ A computer, computer system or ~~computer~~ network.

B. IN ADDITION TO SECTION 13-109, A PROSECUTION FOR A VIOLATION OF THIS SECTION MAY BE TRIED IN ANY OF THE FOLLOWING COUNTIES:

1. THE COUNTY IN WHICH THE VICTIMIZED COMPUTER, COMPUTER SYSTEM OR NETWORK IS LOCATED.

2. THE COUNTY IN WHICH THE COMPUTER, COMPUTER SYSTEM OR NETWORK THAT WAS USED IN THE COMMISSION OF THE OFFENSE IS LOCATED OR IN WHICH ANY BOOKS, RECORDS, DOCUMENTS, PROPERTY, FINANCIAL INSTRUMENTS, COMPUTER SOFTWARE, DATA, ACCESS DEVICES OR INSTRUMENTS OF THE OFFENSE WERE USED.

3. THE COUNTY IN WHICH ANY AUTHORIZED USER WAS DENIED SERVICE OR IN WHICH AN AUTHORIZED USER'S SERVICE WAS INTERRUPTED.

4. THE COUNTY IN WHICH CRITICAL INFRASTRUCTURE RESOURCES WERE TAMPERED WITH OR AFFECTED.

C. ON CONVICTION OF A VIOLATION OF THIS SECTION, THE COURT SHALL ORDER THAT ANY COMPUTER SYSTEM OR INSTRUMENT OF COMMUNICATION THAT WAS OWNED OR USED EXCLUSIVELY BY THE DEFENDANT AND THAT WAS USED IN THE COMMISSION OF THE OFFENSE BE FORFEITED AND SOLD, DESTROYED OR OTHERWISE PROPERLY DISPOSED.

D. A VIOLATION OF SUBSECTION A, PARAGRAPH 6 OF THIS SECTION CONSTITUTES AN UNLAWFUL PRACTICE UNDER SECTION 44-1522 AND IS IN ADDITION TO ALL OTHER CAUSES OF ACTION, REMEDIES AND PENALTIES THAT ARE AVAILABLE TO THIS STATE. THE ATTORNEY GENERAL MAY INVESTIGATE AND TAKE APPROPRIATE ACTION PURSUANT TO TITLE 44, CHAPTER 10, ARTICLE 7.

~~C.~~ E. Computer ~~fraud in the first degree~~ TAMPERING PURSUANT TO SUBSECTION A, PARAGRAPH 1 OF THIS SECTION is a class 3 felony. Computer ~~fraud in the second degree~~ TAMPERING PURSUANT TO SUBSECTION A, PARAGRAPH 2, 3 OR 4 OF THIS SECTION is a class ~~5~~ 4 felony, UNLESS THE COMPUTER, COMPUTER

SYSTEM OR NETWORK TAMPERED WITH IS A CRITICAL INFRASTRUCTURE RESOURCE, IN WHICH CASE IT IS A CLASS 2 FELONY. COMPUTER TAMPERING PURSUANT TO SUBSECTION A, PARAGRAPH 5 OF THIS SECTION IS A CLASS 5 FELONY. COMPUTER TAMPERING PURSUANT TO SUBSECTION A, PARAGRAPH 7 OR 8 OF THIS SECTION IS A CLASS 6 FELONY.

Sec. 11. Title 13, chapter 23, Arizona Revised Statutes, is amended by adding sections 13-2316.01 and 13-2316.02, to read:

13-2316.01. Unlawful possession of an access device; classification

A. A PERSON COMMITS UNLAWFUL POSSESSION OF AN ACCESS DEVICE BY KNOWINGLY POSSESSING, TRAFFICKING IN, PUBLISHING OR CONTROLLING AN ACCESS DEVICE WITHOUT THE CONSENT OF THE ISSUER, OWNER OR AUTHORIZED USER AND WITH THE INTENT TO USE OR DISTRIBUTE THAT ACCESS DEVICE.

B. THE POSSESSION, TRAFFICKING, PUBLISHING OR CONTROL OF FIVE OR MORE ACCESS DEVICES WITHOUT THE CONSENT OF THE ISSUER, OWNER OR AUTHORIZED USER MAY GIVE RISE TO AN INFERENCE THAT THE PERSON POSSESSING, TRAFFICKING IN, PUBLISHING OR CONTROLLING THE ACCESS DEVICES INTENDED TO USE OR DISTRIBUTE THE DEVICES.

C. UNLAWFUL POSSESSION OF ONE HUNDRED OR MORE ACCESS DEVICES IS A CLASS 4 FELONY; UNLAWFUL POSSESSION OF FIVE OR MORE BUT FEWER THAN ONE HUNDRED ACCESS DEVICES IS A CLASS 5 FELONY. UNLAWFUL POSSESSION OF FEWER THAN FIVE ACCESS DEVICES IS A CLASS 6 FELONY.

13-2316.02. Unauthorized release of proprietary or confidential computer security information; exceptions; classification

A. A PERSON COMMITS UNAUTHORIZED RELEASE OF PROPRIETARY OR CONFIDENTIAL COMPUTER SECURITY INFORMATION BY COMMUNICATING, RELEASING OR PUBLISHING PROPRIETARY OR CONFIDENTIAL COMPUTER SECURITY INFORMATION, SECURITY-RELATED MEASURES, ALGORITHMS OR ENCRYPTION DEVICES RELATING TO A PARTICULAR COMPUTER, COMPUTER SYSTEM OR NETWORK WITHOUT THE AUTHORIZATION OF ITS OWNER OR OPERATOR.

B. THE FOLLOWING ARE EXEMPT FROM THIS SECTION:

1. THE RELEASE BY PUBLISHERS, VENDORS, USERS AND RESEARCHERS OF WARNINGS OR INFORMATION ABOUT SECURITY MEASURES OR DEFECTS IN SOFTWARE, HARDWARE OR ENCRYPTION PRODUCTS IF THE RELEASE OF THE WARNINGS OR INFORMATION IS NOT SPECIFIC TO A PARTICULAR OWNER'S OR OPERATOR'S COMPUTER, COMPUTER SYSTEM OR NETWORK.

2. THE RELEASE OF SECURITY INFORMATION AMONG THE AUTHORIZED USERS OF A COMPUTER, COMPUTER SYSTEM OR NETWORK OR THE NOTIFICATION TO THE OWNER OR OPERATOR OF A COMPUTER, COMPUTER SYSTEM OR NETWORK OF A PERCEIVED SECURITY THREAT.

3. THE RELEASE OF SECURITY INFORMATION IN CONNECTION WITH THE RESEARCH, DEVELOPMENT AND TESTING OF SECURITY-RELATED MEASURES, PRODUCTS OR DEVICES IF THE RELEASE OF THE SECURITY INFORMATION IS NOT SPECIFIC TO A PARTICULAR OWNER'S OR OPERATOR'S COMPUTER, COMPUTER SYSTEM OR NETWORK.

C. AT THE CONCLUSION OF ANY GRAND JURY, HEARING OR TRIAL, THE COURT SHALL PRESERVE PURSUANT TO SECTION 44-405 ANY PROPRIETARY COMPUTER SECURITY INFORMATION THAT WAS ADMITTED IN EVIDENCE OR ANY PORTION OF A TRANSCRIPT THAT CONTAINS INFORMATION RELATING TO PROPRIETARY COMPUTER SECURITY INFORMATION.

D. UNAUTHORIZED RELEASE OF PROPRIETARY OR CONFIDENTIAL COMPUTER SECURITY INFORMATION IS A CLASS 6 FELONY, UNLESS THE SECURITY INFORMATION RELATES TO A CRITICAL INFRASTRUCTURE RESOURCE, IN WHICH CASE IT IS A CLASS 4 FELONY.

Sec. 12. Repeal

Sections 13-2912, 13-2913 and 13-2914, Arizona Revised Statutes, are repealed.

Sec. 13. Renumber

Section 13-3001, Arizona Revised Statutes, is renumbered as section 13-3004.

Sec. 14. Section 13-3004, Arizona Revised Statutes, is renumbered as section 13-3001 and, as so renumbered, is amended to read:

13-3001. Definitions

In this chapter, unless the context otherwise requires:

1. "Aural transfer" means a communication containing the human voice at any point between and including the point of origin and the point of reception.

2. "CHILD MONITORING DEVICE" MEANS A DEVICE THAT IS CAPABLE OF TRANSMITTING AN AUDIO OR AUDIOVISUAL SIGNAL AND THAT IS INSTALLED OR USED IN A RESIDENCE FOR CHILD SUPERVISION OR SAFETY MONITORING BY ANY PARENT, GUARDIAN OR OTHER RESPONSIBLE PERSON IN THE PERSON'S OWN RESIDENCE.

~~2.~~ 3. "Communication service provider" means any person engaged in providing a service ~~which~~ THAT allows its users to send or receive ORAL, wire or electronic communications OR COMPUTER SERVICES.

~~3.~~ 4. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature THAT IS transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system but THAT does not include any of the following:

(a) Any wire or oral communication.

(b) Any communication made through a tone-only paging device.

(c) Any communication from a tracking device.

~~4.~~ 5. "Electronic communication system" means any communication or computer facilities or related electronic equipment for the transmission, processing or electronic storage of electronic communications.

~~5.~~ 6. "Electronic storage" means either of the following:

(a) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission.

(b) Any storage of the communication by an electronic communication service provider for purposes of backup protection of the communication.

~~6.~~ 7. "Intercept" means the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.

~~7.~~ 8. "Oral communication" means a spoken communication THAT IS uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying ~~such~~ THE expectation~~,~~ but does not include any electronic communication.

~~8.~~ 9. "Pen register" means a device ~~which~~ THAT records or decodes electronic or other impulses ~~which~~ THAT identify the numbers dialed or otherwise transmitted on the telephone line or communication facility to which the device is attached.

~~9.~~ 10. "Person" means any individual, enterprise, public or private corporation, unincorporated association, partnership, firm, society, governmental authority or entity, including the subscriber to the communication service involved, and any law enforcement officer.

~~10.~~ 11. "Readily accessible to the general public" means a radio communication that is not:

(a) Scrambled or encrypted.

(b) Transmitted using modulation techniques with essential parameters that have been withheld from the public to preserve the privacy of the communication.

(c) Carried on a subcarrier or other signal subsidiary to a radio transmission.

(d) Transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system communication.

(e) Transmitted on frequencies allocated under part 25, subpart D, E or F or part 74 or part 94 of the rules of the federal communications commission. If a communication transmitted on a frequency allocated under part 74 is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication system by radio.

~~11.~~ 12. "Remote computing service" means providing to the public any computer storage or processing services by means of an electronic communication system.

~~12.~~ 13. "Trap and trace device" means a device ~~which~~ THAT captures the incoming electronic or other impulses ~~which~~ THAT identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

~~13.~~ 14. "Wire communication" means any aural transfer ~~which~~ THAT is made in whole or in part through the use of facilities for the transmission of communications by the aid of ANY wire, cable or other like connection between the point of origin and the point of reception, including the use of a connection in a switching station, and that is furnished or operated by any person engaged in providing or operating the facilities for the transmission of communications. Wire communication ~~also~~ includes any electronic storage of the communication.

Sec. 15. Section 13-3008, Arizona Revised Statutes, is amended to read:

13-3008. Possession of interception devices; classification

A. IT IS UNLAWFUL FOR a person ~~who has~~ TO HAVE in his possession or control any device, contrivance, machine or apparatus designed or primarily useful for THE interception of wire, electronic or oral communications as defined in section ~~13-3004, intending~~ 13-3001 WITH THE INTENT to unlawfully use or employ or allow the ~~same~~ DEVICE, CONTRIVANCE, MACHINE OR APPARATUS to be ~~so~~ used or employed for THE interception, or having reason to know the ~~same~~ DEVICE, CONTRIVANCE, MACHINE OR APPARATUS is intended to be so used~~, is guilty of a class 6 felony~~.

B. All property possessed or controlled by any person in violation of this section is subject to seizure and forfeiture pursuant to chapter 39 of this title.

C. A PERSON WHO VIOLATES THIS SECTION IS GUILTY OF A CLASS 6 FELONY.

Sec. 16. Section 13-3010, Arizona Revised Statutes, is amended to read:

13-3010. Ex parte order for interception; definition

A. ~~An ex parte order for interception of wire, electronic or oral communications may be issued by any justice of the supreme court, judge of the court of appeals or judge of the superior court upon~~ ON application of a county attorney, ~~or~~ the attorney general or ~~such~~ a prosecuting ~~attorneys as they may designate in writing, along with the supporting oath or affirmation of the investigating peace officer of the state or of any political subdivision of the state, where~~ ATTORNEY WHOM A COUNTY ATTORNEY OR THE ATTORNEY GENERAL DESIGNATES IN WRITING, ANY JUSTICE OF THE SUPREME COURT, JUDGE OF THE COURT OF APPEALS OR SUPERIOR COURT JUDGE MAY ISSUE AN EX PARTE ORDER FOR THE INTERCEPTION OF WIRE, ELECTRONIC OR ORAL COMMUNICATIONS IF there is probable cause to believe BOTH:

1. ~~That~~ A crime has been, is being or is about to be committed~~, and there is probable cause to believe~~.

2. ~~That~~ Evidence of ~~such~~ THAT crime or the location of a fugitive from justice from that crime may be obtained by THE interception.

B. An application under subsection A shall be made in writing and upon the oath or affirmation of the applicant. It shall include:

1. The name and title of the applicant.

2. A full and complete statement of the facts and circumstances relied upon by the applicant, including the supporting oath or affirmation of the investigating peace officer OF THIS STATE OR ANY POLITICAL SUBDIVISION OF THIS STATE to justify the officer's belief that an order should be issued~~, including~~. THE STATEMENT SHALL INCLUDE:

(a) Details as to the particular crime that has been, is being or is about to be committed.

(b) The identity of the person, if known, committing the offense and whose communications are to be intercepted.

(c) A particular description of the type of communications sought to be intercepted.

(d) A particular description of the nature, identification and location of the communication facility from which or the place where the communication is to be intercepted. If the identification or specific description of the communication facility from which or the place where the communication is to be intercepted is not practical, the affidavit in support of the application must state ~~the reasons~~ why ~~such~~:

(i) Specification is impractical~~, and the reasons why~~.

(ii) Interception from any facility or at any place where the communication may occur is necessary.

3. A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.

4. A statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that authorization to intercept should not automatically terminate when the described type of communication has been first obtained, THE STATEMENT SHALL INCLUDE a particular description of facts establishing probable cause to believe that additional communications of the same type will occur ~~thereafter~~ AFTER THE COMMUNICATION HAS BEEN FIRST OBTAINED.

5. A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each ~~such~~ application.

6. ~~Where~~ IF the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

C. Upon proper application, a judge may enter an ex parte order AUTHORIZING INTERCEPTION, as requested or with any appropriate modifications, ~~authorizing interception~~ if ~~he~~ THE JUDGE determines on the basis of the facts submitted by the applicant that:

1. There is probable cause to believe that a person is committing, has committed~~,~~ or is about to commit a particular crime ~~included within subsection A~~.

2. There is probable cause to believe that particular communications concerning that offense will be obtained through ~~such~~ THE interception.

3. Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.

4. There is probable cause to believe any of the following:

(a) Wire or electronic communications concerning the offense are being made or are about to be made by the person over the communication facilities for which interception authority is granted.

(b) Oral communications concerning the offense are being made or are about to be made by the person in the location for which interception authority is granted.

(c) Communications concerning the offense are being made or are about to be made by the person in different and changing locations, or from different and changing facilities.

D. Each order authorizing the interception of any wire, electronic or oral communication shall specify ALL OF THE FOLLOWING:

1. The identity of the person, if known, whose communications are to be intercepted.

2. The nature and location of the communication facilities as to which~~,~~ or the place where~~,~~ authority to intercept is granted. If authority is granted to intercept communications of a person wherever that person is located or from whatever communication facility is used, the order shall so state and shall include any limitations imposed by the authorizing judge as to location, time or manner of the interception. The order shall state that the interception shall not begin until the facilities from which or the place where the communication is to be intercepted is ascertained by the person implementing the interception order.

3. A particular description of the type of communication sought to be intercepted~~,~~ and a statement of the particular offense to which it relates.

4. The identity of the agency authorized to intercept the communications~~,~~ and of the person authorizing the application.

5. The period of time during which ~~such~~ THE interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

6. That the authorization for interception be executed as soon as practicable, that it be conducted in such a way as to minimize THE interception of communications not otherwise subject to interception under this section and that it ~~shall~~ terminate upon attainment of the authorized objective or on the date specified, whichever comes first.

7. That entry may be made to service, install or remove interception devices or equipment~~,~~ if ~~such~~ entry is necessary to effect the interception.

E. ~~No~~ AN order THAT IS entered under this section may NOT authorize the interception of any wire or oral communication for any period THAT IS longer than is necessary to achieve the objective of the authorization~~, in any event no longer than~~ AND THAT EXCEEDS thirty days. This thirty day period begins on the earlier of the day on which the interception actually begins under the order or ten days after the order is signed. THE COURT MAY GRANT extensions of any order ~~may be granted, but only upon~~ IF AN application for an extension IS made ~~in accordance with~~ PURSUANT TO subsection A and the court ~~making~~ MAKES the findings required by subsection C. The period of extension shall be no longer than the authorizing judge deems necessary to

achieve the purposes for which it was granted and ~~in no event for longer than~~ SHALL NOT EXCEED thirty days.

F. Any ex parte order for interception, together with the papers ~~upon~~ ON which the application was based, shall be delivered to and retained by the applicant during the duration of the interception as authority for the interception authorized ~~therein~~ IN THE ORDER. THE JUSTICE OR JUDGE ISSUING THE ORDER SHALL RETAIN a true copy of ~~such~~ THE order ~~shall~~ at all times ~~be retained by the judge or justice issuing the order~~.

G. WITHIN TEN DAYS after the termination of the authorized interception, applications made and orders granted under this ~~statute~~ SECTION shall ~~within ten days~~ be returned to and sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. ~~Such~~ THE applications and orders shall be disclosed only ~~upon~~ ON a showing of good cause before a judge of competent jurisdiction or as otherwise provided.

H. IF POSSIBLE, the contents of any communication THAT IS intercepted by any means authorized by this ~~statute~~ SECTION shall~~, if possible,~~ be recorded on ANY tape, electronic, wire or other comparable device. The recording of the contents of any wire, electronic or oral communication under this subsection shall be done in such a way as will protect the recording from editing or alterations. Within ten days after the termination of the authorized interception, ~~such~~ THE recordings shall be made available to the judge ~~issuing such~~ WHO ISSUED THE order and SHALL BE sealed under the judge's directions. Custody of the recordings shall be maintained pursuant to court order. The recordings shall BE KEPT FOR TEN YEARS AND SHALL not be destroyed except on an order of the issuing judge or ~~other~~ ANOTHER judge of competent jurisdiction ~~and in any event shall be kept for ten years~~.

I. Within ninety days after an application under subsection A is denied, or the period of an order or ~~extensions thereof~~ ANY EXTENSION expires, the issuing or denying judge shall ~~cause~~ SERVE the persons named in the order or application~~,~~ and ~~such~~ ANY other parties to THE intercepted communications as the judge may determine the interests of justice require~~, to be served~~ with an inventory, including notice of all of the following:

1. The fact of the entry of the order or the application.

2. The date of the entry and the period of authorized interception, or the denial of the application.

3. The fact that during the period OF AUTHORIZED INTERCEPTION wire, electronic or oral communications were or were not intercepted. On motion, the judge may ~~in the judge's discretion~~ make available to ~~such~~ THE person or the person's ~~counsel~~ ATTORNEY for inspection such portions of the intercepted communications, applications and order as the judge determines to be in the interest of justice. On an ex parte showing of good cause to the judge, the serving of the notice required by this subsection may be postponed.

J. ON REQUEST OF THE APPLICANT, any order authorizing interception shall~~, upon the request of the applicant,~~ direct that the communication service provider, landlords, custodians or other persons furnish the

applicant with all information, facilities~~,~~ and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that ~~such~~ THESE persons are according the person whose communications are to be intercepted.

K. The order may require written reports to be made to the issuing judge at specified intervals showing the progress made toward achieving the authorized objective and the need for continued interception.

L. Any order authorizing THE interception of wire communications pursuant to this chapter is also deemed to authorize THE interception of any electronic communication ~~which~~ THAT may be made over the same equipment or by the same facility.

M. If the intercepted communication is in a code or foreign language and an expert in that code or foreign language is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after ~~such~~ THE interception.

N. An interception under this chapter may be conducted in whole or in part by government personnel or by an individual operating under a contract with the government or acting under the supervision of a law enforcement officer WHO IS authorized to conduct the interception.

O. The applicant is responsible for providing to the administrative office of the United States courts all reports on applications for or ~~interception~~ INTERCEPTIONS of wire, electronic or oral communications THAT ARE required by federal statutes.

P. For the purposes of this section, "crime" means murder, gaming, kidnapping, robbery, bribery, extortion, theft, ~~offenses defined in~~ AN ACT IN VIOLATION OF chapter 23 of this title, dealing in narcotic drugs, marijuana or dangerous drugs, SEXUAL EXPLOITATION OF CHILDREN IN VIOLATION OF CHAPTER 35.1 OF THIS TITLE or any felony that is dangerous to life, limb or property ~~or any~~. CRIME INCLUDES conspiracy to commit any of the offenses listed in this subsection.

Sec. 17. Section 13-3011, Arizona Revised Statutes, is amended to read:

13-3011. Disclosing confidential information relating to ex parte order; exceptions; classification

A. Except in any trial, hearing or other judicial proceeding, a person ~~who~~ SHALL NOT knowingly ~~discloses~~ DISCLOSE to ~~any~~ ANOTHER person~~, other than the communication service provider whose facilities are involved, or an employee or other authorized agent of the county attorney, attorney general, sheriff or police officer making application for an order permitting interception or installation of a pen register or trap and trace device,~~ any information concerning EITHER:

1. The application for~~,~~ OR the granting or denial of orders for THE interception or installation of a pen register or trap and trace device~~,~~ or A REQUEST FOR THE PRESERVATION OF RECORDS OR EVIDENCE PURSUANT TO SECTION 13-3016 OR A SUBPOENA ISSUED PURSUANT TO SECTION 13-3018.

2. The identity of the person or persons whose communications are the subject of an ex parte order, SUBPOENA OR RECORDS PRESERVATION REQUEST granted pursuant to sections 13-3010, 13-3015, 13-3016, ~~and~~ 13-3017 ~~shall be guilty of a class 1 misdemeanor~~ AND 13-3018.

B. SUBSECTION A OF THIS SECTION DOES NOT APPLY TO THE DISCLOSURE OF INFORMATION TO THE COMMUNICATION SERVICE PROVIDER WHOSE FACILITIES ARE INVOLVED OR TO AN EMPLOYEE OR OTHER AUTHORIZED AGENT OF THE COUNTY ATTORNEY, ATTORNEY GENERAL OR LAW ENFORCEMENT AGENCY THAT APPLIES FOR AN ORDER PERMITTING INTERCEPTION OR INSTALLATION OF A PEN REGISTER OR TRAP AND TRACE DEVICE OR WHO REQUESTS THE PRESERVATION OF RECORDS OR EVIDENCE PURSUANT TO SECTION 13-3016 OR A SUBPOENA ISSUED PURSUANT TO SECTION 13-3018.

~~B.~~ C. Notwithstanding subsection A of this section, a peace officer or prosecuting attorney who~~, by any means authorized by sections 13-3010, 13-3015, 13-3016 and 13-3017,~~ obtains knowledge of the contents of a wire, electronic or oral communication~~,~~ AS AUTHORIZED BY SECTIONS 13-3010, 13-3015, 13-3016, 13-3017 AND 13-3018 or evidence derived from ~~such~~ THAT knowledge~~,~~ may:

1. Disclose the contents of the communication to a peace officer or prosecuting attorney to the extent the disclosure is appropriate to the proper performance of the official duties of the peace officer or prosecuting attorney making or receiving the disclosure.

2. Use the contents of the communication to the extent THAT the use is appropriate to the proper performance of the official duties of the peace officer or prosecuting attorney.

D. A PERSON WHO VIOLATES THIS SECTION IS GUILTY OF A CLASS 1 MISDEMEANOR.

Sec. 18. Section 13-3012, Arizona Revised Statutes, is amended to read:

13-3012. Exemptions

The following are exempt from the provisions of this chapter:

1. THE interception of wire, electronic or oral communications, THE installation and operation of a pen register or trap and trace device, ~~or~~ THE providing of information, facilities or technical assistance to an investigative or law enforcement officer pursuant to a subpoena or an ex parte order granted pursuant to sections 13-3010, 13-3015, 13-3016, ~~and~~ 13-3017 AND 13-3018 or an emergency interception made in good faith pursuant to section 13-3015, including any of the foregoing acts by a communication service provider or its officers, agents or employees.

2. The normal use of services, equipment and facilities THAT ARE provided by a communication service provider pursuant to tariffs on file with the ARIZONA corporation commission ~~of the state of Arizona~~ or the federal communications commission and the normal functions of any operator of a switchboard.

3. Any officer, agent or employee of a communication service provider who performs acts THAT ARE otherwise prohibited by this article in providing,

constructing, maintaining, repairing, operating or using the provider's services, equipment or facilities, protecting the provider's service, equipment and facilities from illegal use in violation of tariffs on file with the ARIZONA corporation commission ~~of this state~~ or the federal communications commission and protecting the provider from the commission of fraud against it.

4. Providing requested information or ANY other response to a subpoena or other order issued by a court of competent jurisdiction or on demand of ANY other lawful authority.

5. THE interception of wire or electronic communications or the use of a pen register or trap and trace device ~~in any of the following instances~~ BY A COMMUNICATION SERVICE PROVIDER IF THE INTERCEPTION OR USE EITHER:

(a) ~~By a provider of a wire or electronic communication service relating~~ RELATES to the operation, maintenance and testing of that service, ~~relating to~~ the protection of the rights or property of the provider or ~~relating to~~ the protection of users of that service from fraudulent, abusive or unlawful use of that service.

(b) ~~By a provider of a wire or electronic communication service to record~~ RECORDS the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the communication~~,~~ or a user of that service from fraudulent, unlawful or abusive use of that service.

~~(c) If consent of the user or subscriber of that service has been obtained.~~

6. The interception of any radio communication that is transmitted:

(a) By any station for the use of the general public or if the transmission relates to ships, aircraft, vehicles or persons in distress.

(b) By any government, law enforcement, civil defense, private land mobile or public safety communication system, including police and fire systems, AND that ~~are~~ IS readily accessible to the general public.

(c) By any station that operates on an authorized frequency within the bands that are allocated to the amateur, citizens band or general mobile radio services.

(d) By any marine or aeronautical communications system.

(e) Through a system using frequencies that are monitored by persons who are engaged in the provision or the use of the system or by other persons using the same frequency if the communication is not scrambled or encrypted.

7. THE interception of wire or electronic communication if the transmission is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of the interference.

8. The use of a pen register or trap and trace device by a ~~provider or subscriber of a wire or electronic~~ communication service PROVIDER for billing or recording as an incident to billing for communication services,

or for cost accounting or other like purposes in the ordinary course of business.

9. The interception of any wire, electronic or oral communication by any person, if the interception is effected with the consent of a party to the communication or a person WHO IS present during the communication, OR THE INSTALLATION OF A PEN REGISTER OR TRAP AND TRACE DEVICE WITH THE CONSENT OF A USER OR SUBSCRIBER TO THE SERVICE.

10. Divulging the contents of a wire or electronic communication to a law enforcement agency by a remote computing service or communication service provider, officer or employee if ~~such~~ THE contents were lawfully or inadvertently obtained by the service provider and appear to pertain to the commission of a crime.

11. The interception or access of AN electronic communication THAT IS made through an electronic communication system AND that is configured so that the electronic communication is readily accessible to the general public.

~~12. The interception of radio communication that is transmitted:~~

~~(a) By a station for the use of the general public or ships, aircraft, vehicles or persons in distress.~~

~~(b) By a governmental, law enforcement, civil defense, private land, mobile or public safety communications system, including police and fire.~~

~~(c) By a station operating on an authorized frequency within the bands allocated to the amateur, citizens band or general mobile radio services.~~

~~(d) By a marine or aeronautical communications system.~~

~~13. The interception of a wire or electronic communication the transmission of which is causing harmful interference to a lawfully operating station or consumer electronic equipment to identify the source of this interference.~~

~~14.~~ 12. For other users of the same frequency to intercept a radio communication THAT IS made through a system that uses frequencies monitored by individuals who provide or use the system, if the communication is not scrambled or encrypted.

13. THE INTERCEPTION OF ORAL COMMUNICATIONS BY MEANS OF A CHILD MONITORING DEVICE.

Sec. 19. Section 13-3013, Arizona Revised Statutes, is amended to read:

13-3013. Defenses

THE FOLLOWING CONSTITUTE A COMPLETE DEFENSE TO ANY CIVIL OR CRIMINAL ACTION BROUGHT UNDER THIS CHAPTER OR UNDER ANY OTHER LAW:

1. A good faith reliance on an ex parte order or subpoena THAT IS issued pursuant to section 13-3010, 13-3015, 13-3016, ~~or~~ 13-3017 OR 13-3018~~,~~ ~~or~~.

2. Providing information pursuant to section 13-3012~~, or~~.

3. Providing assistance, information or facilities for an emergency interception pursuant to section 13-3015~~, or~~.

4. Disclosing stored electronic communications or ~~creating and delivering a backup copy~~ PRESERVING RECORDS, CONTENT OR EVIDENCE pursuant to section 13-3016~~, or~~.

5. Providing equipment, information or assistance to render stored electronic communications ~~or a backup copy~~ in a usable form pursuant to section 13-3016~~, shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law~~.

Sec. 20. Section 13-3016, Arizona Revised Statutes, is amended to read:

13-3016. Stored oral, wire and electronic communications; agency access; backup preservation; delayed notice; records preservation request; violation; classification

A. ~~The provisions of~~ This section ~~apply~~ APPLIES to ORAL, WIRE AND electronic communications THAT ARE entrusted to a communication service provider or remote computing service solely for the purpose of transmission, storage or processing. ORAL, WIRE AND electronic communications THAT ARE in the possession of a person who is entitled to access the contents of such communications for any purpose other than transmission, storage or processing are ordinary business records~~, and~~ THAT may be obtained by subpoena or court order.

B. An agency OR POLITICAL SUBDIVISION of this state ~~or its political subdivisions~~ may require the disclosure by a COMMUNICATION SERVICE provider ~~of electronic communication services~~ OR REMOTE COMPUTING SERVICE of the contents of an ORAL, WIRE OR electronic communication that has been in electronic storage for one hundred eighty days or less ~~only by obtaining a search warrant pursuant to chapter 38 of this title.~~ IN ONE OF THE FOLLOWING WAYS:

1. WITHOUT PRIOR NOTICE TO THE SUBSCRIBER OR PARTY, BY OBTAINING A SEARCH WARRANT ISSUED PURSUANT TO CHAPTER 38, ARTICLE 8 OF THIS TITLE.

2 WITH PRIOR NOTICE TO THE SUBSCRIBER OR PARTY, BY SERVING A SUBPOENA, EXCEPT THAT NOTICE MAY BE DELAYED PURSUANT TO SUBSECTION D OF THIS SECTION.

3. WITH PRIOR NOTICE TO THE SUBSCRIBER OR PARTY, BY OBTAINING A COURT ORDER ON AN APPLICATION AND CERTIFICATION THAT CONTAINS SPECIFIC AND ARTICULABLE FACTS SHOWING THAT THERE ARE REASONABLE GROUNDS TO BELIEVE THAT THE COMMUNICATION CONTENT SOUGHT IS RELEVANT TO AN ONGOING CRIMINAL INVESTIGATION, EXCEPT THAT NOTICE MAY BE DELAYED PURSUANT TO SUBSECTION D OF THIS SECTION.

C. An agency OR POLITICAL SUBDIVISION of this state ~~or its political subdivisions~~ may require the disclosure by a COMMUNICATION SERVICE provider ~~of electronic communication services~~ OR REMOTE COMPUTING SERVICE of the contents of an ORAL, WIRE OR electronic communication that has been in electronic storage for more than one hundred eighty days IN ONE OF THE FOLLOWING WAYS:

1. Without notice to the subscriber or ~~customer~~ PARTY, by obtaining a search warrant issued pursuant to chapter 38, ARTICLE 8 of this title.

2. With prior notice to the subscriber or ~~customer~~ PARTY, by SERVING A subpoena, except that ~~such~~ notice may be delayed pursuant to subsection ~~E~~ D OF THIS SECTION.

3. With prior notice to the subscriber or ~~customer if the agency obtains~~ PARTY, BY OBTAINING a court order on AN application and certification ~~to the court that the information likely to be obtained is relevant to a legitimate law enforcement inquiry~~ THAT CONTAINS SPECIFIC AND ARTICULABLE FACTS SHOWING THAT THERE ARE REASONABLE GROUNDS TO BELIEVE THAT THE COMMUNICATION CONTENT SOUGHT IS RELEVANT TO AN ONGOING CRIMINAL INVESTIGATION, except that ~~such~~ notice may be delayed pursuant to subsection ~~E~~ D OF THIS SECTION.

~~D. An agency of this state or its political subdivisions may require a provider of remote computing services to disclose the contents of any electronic communication that is held or maintained on that service on behalf of a subscriber or customer of the remote computing service solely for the purpose of providing storage or computer processing services to the subscriber or customer:~~

~~1. Without notice to the subscriber or customer, by obtaining a search warrant issued pursuant to chapter 38 of this title.~~

~~2. With prior notice to the subscriber or customer, by subpoena, except that such notice may be delayed pursuant to subsection E.~~

~~3. With prior notice to the subscriber or customer if the agency obtains a court order on application and certification to the court that the information likely to be obtained is relevant to a legitimate law enforcement inquiry, except that such notice may be delayed pursuant to subsection E.~~

~~E. An agency acting pursuant to this section may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications:~~

~~1. Without notifying the subscriber or customer, the provider shall:~~

~~(a) Create the backup copy as soon as practicable but in no event no later than two business days after receipt of the subpoena or order.~~

~~(b) Confirm to the requesting agency that the backup copy has been made.~~

~~(c) Promptly deliver the backup copy to the court issuing the subpoena or order.~~

~~2. The court shall seal and retain the backup copy or make such other provision as it deems necessary to ensure that the backup copy is preserved until resolution of any proceedings pursuant to this section.~~

~~3. Within three days after receipt of confirmation, the agency shall notify the subscriber or customer of the creation of the backup copy, except that notice may be delayed pursuant to this subsection.~~

~~4. Within fourteen days after notice by the agency, the subscriber or customer may challenge the agency's request by filing an application to quash the subpoena or vacate the court order and serving the requesting agency.~~

~~5. If after response by the agency and such further proceedings as the court may deem necessary, the court finds that the applicant is not the subscriber or customer for whom the communications sought by the agency are maintained by the provider, or that there is reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, the court shall deny the application and deliver the backup copy to the requesting agency. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the agency are maintained, and that there is no reason to believe the communications sought are relevant to a legitimate law enforcement inquiry, the court shall grant the application and order the backup copy to be destroyed.~~

~~6. The court shall release the backup copy to the requesting agency no sooner than fourteen days after the agency's notice to the subscriber or customer if the subscriber or customer has not filed a challenge to the subpoena or court order.~~

~~7. The court shall not destroy the backup copy until the information requested is delivered or until the resolution of any proceedings arising from a challenge to the subpoena or order.~~

~~F.~~ D. EXCEPT AS PROVIDED IN SUBSECTION E OF THIS SECTION, THE notice to the subscriber or ~~customer~~ PARTY THAT IS required by this section may be delayed for a period of not to exceed ninety days under any of the following circumstances:

1. If the applicant for a search warrant or court order pursuant to this section requests a delay of notification and the court finds that ~~such~~ delay is necessary to protect the safety of any person or to prevent flight from prosecution, tampering with evidence, intimidation of witnesses or jeopardizing an investigation.

2. If the investigator or prosecuting attorney proceeding by subpoena executes a written certification that there is reason to believe that notice to the subscriber or ~~customer~~ PARTY may result in danger to the safety of any person, flight from prosecution, tampering with evidence, intimidation of witnesses or jeopardizing an investigation. The agency shall retain a true copy of the certification WITH THE SUBPOENA.

~~3.~~ E. If further delay of notification is necessary, extensions of up to ninety days each may be obtained by application to the court or certification pursuant to ~~paragraphs 1 and 2 of this~~ subsection D OF THIS SECTION.

~~4.~~ F. Any agency acting pursuant to this section may apply for a court order directing the communication ~~or computing~~ service provider OR REMOTE COMPUTING SERVICE not to notify any other person of the existence of the subpoena, court order or warrant for such period as the court deems appropriate. The court shall grant the application if it finds that there

is reason to believe that notice may cause an adverse result described in ~~paragraphs 1 and 2 of this~~ subsection D OF THIS SECTION. A person who violates an order issued pursuant to this subsection is guilty of a class 1 misdemeanor.

~~5.~~ G. On the expiration of any period of delay under this section, the agency shall deliver to the subscriber or ~~customer~~ PARTY a copy of the process used and notice including:

~~(a)~~ 1. That information was requested from the service provider.

~~(b)~~ 2. The date on which the information was requested.

~~(c)~~ 3. That notification to the subscriber or ~~customer~~ PARTY was delayed.

~~(d)~~ 4. The identity of the court or agency ordering or certifying the delay.

~~(e)~~ 5. The provision of this section by which delay was obtained.

~~(f)~~ 6. That any challenge to the subpoena or order must be filed within fourteen days.

H. ON THE REQUEST OF AN AGENCY OR POLITICAL SUBDIVISION OF THIS STATE, A COMMUNICATION SERVICE PROVIDER OR REMOTE COMPUTING SERVICE SHALL TAKE ALL NECESSARY STEPS TO PRESERVE RECORDS, COMMUNICATION CONTENT AND OTHER EVIDENCE IN ITS POSSESSION PENDING THE ISSUANCE OF A COURT ORDER OR OTHER PROCESS. THE COMMUNICATION SERVICE PROVIDER OR REMOTE COMPUTING SERVICE SHALL RETAIN THE PRESERVED RECORDS, COMMUNICATION CONTENT AND OTHER EVIDENCE FOR NINETY DAYS. ON THE RENEWED REQUEST OF AN AGENCY OR POLITICAL SUBDIVISION, THE PRESERVATION PERIOD MAY BE EXTENDED FOR AN ADDITIONAL NINETY DAYS. EXCEPT AS PROVIDED IN SECTION 13-3011, A PERSON SHALL NOT NOTIFY THE SUBSCRIBER OR PARTY DURING THE PERIOD OF THE PRESERVATION REQUEST.

Sec. 21. Renumber

Section 13-3018, Arizona Revised Statutes, is renumbered as section 13-3019.

Sec. 22. Title 13, chapter 30, Arizona Revised Statutes, is amended by adding a new section 13-3018, to read:

13-3018. Communication service records; subpoenas; application; certification; definition

A. THIS SECTION APPLIES TO ALL COMMUNICATION SERVICE PROVIDERS THAT DO BUSINESS IN THIS STATE OR THAT FURNISH COMMUNICATION SERVICES TO PERSONS WITHIN THIS STATE.

B. THE PROSECUTOR MAY ISSUE A SUBPOENA DUCES TECUM TO A COMMUNICATION SERVICE PROVIDER IN ORDER TO OBTAIN COMMUNICATION SERVICE RECORDS IN CONNECTION WITH A CRIMINAL INVESTIGATION OR PROSECUTION FOR ANY OFFENSE IN WHICH A PROSECUTOR SUSPECTS THAT A COMPUTER OR NETWORK WAS USED. THIS SUBSECTION DOES NOT PREVENT THE PROSECUTOR FROM OBTAINING A GRAND JURY SUBPOENA DUCES TECUM.

C. THE PROSECUTOR WHO ISSUES A SUBPOENA PURSUANT TO THIS SECTION SHALL CERTIFY IN THE BODY OF THE SUBPOENA THAT THE INFORMATION LIKELY TO BE OBTAINED IS RELEVANT TO AN ONGOING CRIMINAL INVESTIGATION.

D. AN AUTHORIZED REPRESENTATIVE OF A COMMUNICATION SERVICE PROVIDER MAY CERTIFY COMMUNICATION SERVICE RECORDS THAT ARE OBTAINED BY SUBPOENA IF ALL OF THE FOLLOWING APPLY:

1. THE RECORDS ARE THE REGULAR COMMUNICATION SERVICE RECORDS THAT ARE USED AND KEPT BY THE COMMUNICATION SERVICE PROVIDER.

2. THE RECORDS ARE MADE AT OR NEAR THE TIME THE UNDERLYING COMMUNICATIONS OCCUR IN THE ORDINARY COURSE OF BUSINESS.

3. THE AUTHORIZED REPRESENTATIVE CERTIFIES THAT THE RECORD PRODUCED IN RESPONSE TO THE SUBPOENA IS AN ACCURATE COPY OF THE COMMUNICATION SERVICE PROVIDER RECORDS.

E. CERTIFIED COMMUNICATION SERVICE RECORDS THAT ARE OBTAINED BY SUBPOENA MAY BE INTRODUCED IN EVIDENCE AT A HEARING OR TRIAL AND CONSTITUTE PRIMA FACIE EVIDENCE OF THE FACTS CONTAINED IN THE RECORDS.

F. IF A CERTIFICATION OF COMMUNICATION SERVICE PROVIDER RECORDS IS ACKNOWLEDGED BY ANY NOTARY OR OTHER OFFICER WHO IS AUTHORIZED BY LAW TO TAKE ACKNOWLEDGMENTS, THE CERTIFICATION SHALL BE RECEIVED IN EVIDENCE WITHOUT FURTHER PROOF OF ITS AUTHENTICITY.

G. FOR THE PURPOSES OF THIS SECTION, "COMMUNICATION SERVICE RECORDS" INCLUDES SUBSCRIBER INFORMATION, INCLUDING NAME, BILLING OR INSTALLATION ADDRESS, LENGTH OF SERVICE, PAYMENT METHOD, TELEPHONE NUMBER, ELECTRONIC ACCOUNT IDENTIFICATION AND ASSOCIATED SCREEN NAMES, TOLL BILLS OR ACCESS LOGS, RECORDS OF THE PATH OF AN ELECTRONIC COMMUNICATION BETWEEN THE POINT OF ORIGIN AND THE POINT OF DELIVERY AND THE NATURE OF THE COMMUNICATION SERVICE PROVIDED, SUCH AS CALLER IDENTIFICATION, AUTOMATIC NUMBER IDENTIFICATION, VOICE MAIL, ELECTRONIC MAIL, PAGING OR OTHER SERVICE FEATURES. COMMUNICATION SERVICE RECORDS DO NOT INCLUDE THE CONTENT OF ANY STORED ORAL, WIRE OR ELECTRONIC COMMUNICATION.

Sec. 23. Section 13-3019, Arizona Revised Statutes, as renumbered by this act, is amended to read:

13-3019. Surreptitious photographing, videotaping, filming or digitally recording; exemptions; violation; classification; definitions

A. It is unlawful for any person to knowingly photograph, videotape, film, digitally record or by any other means USE A DEVICE TO secretly view or record another person without that person's consent under both of the following circumstances:

1. In a restroom, bathroom, locker room, bedroom or other location where the person has a reasonable expectation of privacy.

2. While the person is urinating, defecating, dressing, undressing, nude or involved in sexual intercourse or sexual contact.

B. It is unlawful to disclose, display, distribute or publish a photograph, videotape, film or digital recording made in violation of subsection A of this section without the consent of the person depicted.

C. This section does not apply to:

1. Photographing, videotaping, filming or digitally recording for security purposes where notice of the use of photographing, videotaping, filming or digital recording equipment is clearly posted in the location.~~;~~

2. Photographing, videotaping, filming or digitally recording by correctional officials for security reasons or in connection with the investigation of alleged misconduct of persons on the premises of a jail or prison.~~; or~~

3. Photographing, videotaping, filming or digitally recording by law enforcement officers pursuant to an investigation, which is otherwise lawful.

4. THE USE OF A CHILD MONITORING DEVICE AS DEFINED IN SECTION 13-3001.

D. A violation of subsection A or B of this section is a class 5 felony.

E. For THE purposes of this section "sexual contact" and "sexual intercourse" have the same ~~meaning as~~ MEANINGS prescribed in section 13-1401.

Sec. 24. Section 13-3417, Arizona Revised Statutes, is amended to read:

13-3417. Use of wire communication or electronic communication in drug related transactions; classification

A. It is unlawful for a person to use any wire communication or electronic communication as defined in section ~~13-3004~~ 13-3001 to facilitate the violation of any felony provision or to conspire to commit any felony provision of this chapter or chapter 23 of this title.

B. Any offense committed by use of a wire communication or electronic communication as set forth in this section is deemed to have been committed at the place where the transmission or transmissions originated or at the place where the transmission or transmissions were received.

C. A person who violates this section is guilty of a class 4 felony except if the felony facilitated carries a class 5 or 6 designation in which case a violation of this section shall carry the same classification as the felony facilitated.

Sec. 25. Section 13-3506, Arizona Revised Statutes, is amended to read:

13-3506. Obscene or harmful items; minors; classification

A. It is unlawful for any person, with knowledge of the character of the item involved, to recklessly TRANSMIT, furnish, present, provide, make available, give, lend, show, advertise, OFFER or distribute to minors any item ~~which~~ THAT is harmful to minors.

B. IN AN ACTION FOR A VIOLATION OF THIS SECTION, PROOF OF ANY OF THE FOLLOWING MAY GIVE RISE TO AN INFERENCE THAT THE PERSON KNEW OR SHOULD HAVE KNOWN THAT THE RECIPIENT OF AN ADVERTISEMENT OR OFFER WAS A MINOR:

1. THE NAME, ACCOUNT, PROFILE, WEB PAGE OR ADDRESS OF THE RECIPIENT CONTAINED INDICIA THAT THE RECIPIENT IS A MINOR.

2. THE RECIPIENT OR ANOTHER PERSON PREVIOUSLY NOTIFIED THE PERSON BY ANY REASONABLE MEANS THAT THE RECIPIENT IS A MINOR.

3. THE RECIPIENT'S ELECTRONIC MAIL OR WEB PAGE CONTAINS INDICIA THAT THE ADDRESS OR DOMAIN NAME IS THE PROPERTY OF, OR THAT THE VISUAL DEPICTION ULTIMATELY WILL BE STORED AT, A SCHOOL AS DEFINED IN SECTION 13-609.

~~B.~~ C. A violation of ~~any provision of~~ this section is a class 4 felony.

Sec. 26. Repeal

Section 13-3508, Arizona Revised Statutes, is repealed.

Sec. 27. Section 13-3551, Arizona Revised Statutes, is amended to read:

13-3551. Definitions

In this chapter, unless the context otherwise requires:

1. "COMMUNICATION SERVICE PROVIDER" HAS THE SAME MEANING PRESCRIBED IN SECTION 13-3004.

2. "COMPUTER" HAS THE SAME MEANING PRESCRIBED IN SECTION 13-2301, SUBSECTION E.

3. "COMPUTER SYSTEM" HAS THE SAME MEANING PRESCRIBED IN SECTION 13-2301, SUBSECTION E.

~~1.~~ 4. "Exploitive exhibition" means the actual or simulated exhibition of the genitals or pubic or rectal areas of any person for the purpose of sexual stimulation of the viewer.

5. "NETWORK" HAS THE SAME MEANING PRESCRIBED IN SECTION 13-2301, SUBSECTION E.

~~2.~~ 6. "Producing" means financing, directing, manufacturing, issuing, publishing or advertising for pecuniary gain.

7. "REMOTE COMPUTING SERVICE" HAS THE SAME MEANING PRESCRIBED IN SECTION 13-3004.

~~3.~~ 8. "Sexual conduct" means actual or simulated:

(a) Sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, whether between persons of the same or opposite sex.

(b) Penetration of the vagina or rectum by any object except when done as part of a recognized medical procedure.

(c) Sexual bestiality.

(d) Masturbation, for the purpose of sexual stimulation of the viewer.

(e) Sadomasochistic abuse for the purpose of sexual stimulation of the viewer.

(f) Defecation or urination for the purpose of sexual stimulation of the viewer.

~~4.~~ 9. "Simulated" means any depicting of the genitals or rectal areas ~~which~~ THAT gives the appearance of sexual conduct or incipient sexual conduct.

~~5.~~ 10. "Visual depiction" includes each visual image that is contained in an undeveloped film, videotape or photograph or data stored in any form and that is capable of conversion into a visual image.

Sec. 28. Section 13-3553, Arizona Revised Statutes, is amended to read:

13-3553. Sexual exploitation of a minor; evidence; exemption; classification

A. A person commits sexual exploitation of a minor by knowingly:

1. Recording, filming, photographing, developing or duplicating any visual depiction in which minors are engaged in exploitive exhibition or other sexual conduct.

2. Distributing, transporting, exhibiting, receiving, selling, purchasing, electronically transmitting, possessing or exchanging any visual depiction in which minors are engaged in exploitive exhibition or other sexual conduct.

B. IF ANY VISUAL DEPICTION OF SEXUAL EXPLOITATION OF A MINOR IS ADMITTED INTO EVIDENCE, THE COURT SHALL SEAL THAT EVIDENCE AT THE CONCLUSION OF ANY GRAND JURY PROCEEDING, HEARING OR TRIAL.

~~B.~~ C. Sexual exploitation of a minor is a class 2 felony and if the minor is under fifteen years of age it is punishable pursuant to section 13-604.01.

Sec. 29. Renumber

Sections 13-3554, 13-3555 and 13-3556, Arizona Revised Statutes, are renumbered as sections 13-3555, 13-3556 and 13-3558, respectively.

Sec. 30. Title 13, chapter 35.1, Arizona Revised Statutes, is amended by adding a new section 13-3554, to read:

13-3554. Luring a minor for sexual exploitation; classification

A. A PERSON COMMITS LURING A MINOR FOR SEXUAL EXPLOITATION BY OFFERING OR SOLICITING SEXUAL CONDUCT WITH ANOTHER PERSON KNOWING OR HAVING REASON TO KNOW THAT THE OTHER PERSON IS A MINOR.

B. IT IS NOT A DEFENSE TO A PROSECUTION FOR A VIOLATION OF THIS SECTION THAT THE OTHER PERSON WAS A PEACE OFFICER POSING AS A MINOR.

C. LURING A MINOR FOR SEXUAL EXPLOITATION IS A CLASS 3 FELONY, AND IF THE MINOR IS UNDER FIFTEEN YEARS OF AGE IT IS PUNISHABLE PURSUANT TO SECTION 13-604.01.

Sec. 31. Title 13, chapter 35.1, Arizona Revised Statutes, is amended by adding sections 13-3557 and 13-3559, to read:

13-3557. Equipment; forfeiture

ON THE CONVICTION OF A PERSON FOR A VIOLATION OF SECTION 13-3552, 13-3553 OR 13-3554, THE COURT SHALL ORDER THAT ANY PHOTOGRAPHIC EQUIPMENT, COMPUTER SYSTEM OR INSTRUMENT OF COMMUNICATION THAT IS OWNED OR USED EXCLUSIVELY BY THE PERSON AND THAT WAS USED IN THE COMMISSION OF THE OFFENSE BE FORFEITED AND SOLD, DESTROYED OR OTHERWISE PROPERLY DISPOSED.

13-3559. Reporting suspected visual depictions of sexual exploitation of a minor; immunity

A. ANY COMMUNICATION SERVICE PROVIDER, REMOTE COMPUTING SERVICE, SYSTEM ADMINISTRATOR, COMPUTER REPAIR TECHNICIAN OR OTHER PERSON WHO DISCOVERS SUSPECTED VISUAL DEPICTIONS OF SEXUAL EXPLOITATION OF A MINOR ON

A COMPUTER, COMPUTER SYSTEM OR NETWORK OR IN ANY OTHER STORAGE MEDIUM MAY REPORT THAT DISCOVERY TO A LAW ENFORCEMENT OFFICER.

B. A PERSON WHO ON DISCOVERY IN GOOD FAITH REPORTS THE DISCOVERY OF SUSPECTED VISUAL DEPICTIONS OF SEXUAL EXPLOITATION OF A MINOR IS IMMUNE FROM CIVIL LIABILITY.

C. IT IS AN AFFIRMATIVE DEFENSE TO A PROSECUTION FOR A VIOLATION OF SECTION 13-3553 THAT ON DISCOVERY A PERSON IN GOOD FAITH REPORTS THE DISCOVERY OF UNSOLICITED SUSPECTED VISUAL DEPICTIONS INVOLVING THE SEXUAL EXPLOITATION OF A MINOR.

Sec. 32. Section 13-3707, Arizona Revised Statutes, is amended to read:

13-3707. Telecommunication fraud; classification; definitions

A. A person commits telecommunication fraud if the person does any of the following:

1. With the intent to defraud another of the lawful charge for telecommunication service, obtains or attempts to obtain any telecommunication service by:

(a) Charging or attempting to charge ~~such~~ THE TELECOMMUNICATION service EITHER:

(i) To an existing ELECTRONIC MAIL ADDRESS, telephone number or credit card number without the authority of the person to whom issued or the subscriber ~~thereto~~ TO or the lawful holder ~~thereof, or~~ OF THE ADDRESS OR NUMBER.

(ii) To a nonexistent, counterfeit, revoked or canceled credit card number~~, or by~~.

(b) Any method of code calling~~, or by~~.

(c) Installing, rearranging~~,~~ or tampering with any facility or equipment~~, or by~~.

(d) The use of any other fraudulent means, method, trick or device.

2. WITH THE INTENT THAT THE SAME BE USED OR EMPLOYED TO EVADE A LAWFUL CHARGE FOR ANY TELECOMMUNICATION SERVICE, sells, rents, lends, gives or otherwise transfers or discloses or attempts to transfer or disclose to another, or offers or advertises for sale or rental, the number or code of an existing, canceled, revoked or nonexistent ELECTRONIC MAIL ADDRESS, telephone number or credit card number or THE method of numbering or coding ~~which~~ THAT is employed in the issuance of telephone numbers, account identification codes or credit card numbers ~~with intent that the same be used or employed to evade a lawful charge for any telecommunication service~~.

3. Knowingly makes, constructs, manufactures, fabricates, erects, assembles or possesses any SOFTWARE, instrument, apparatus, equipment or device, or any part ~~thereof~~ OF ANY SOFTWARE, INSTRUMENT, APPARATUS, EQUIPMENT OR DEVICE, THAT IS designed~~,~~ OR adapted or ~~which~~ THAT can be used EITHER:

(a) To obtain telecommunication service by fraud in violation of THIS subsection ~~A of this section; or~~.

(b) To conceal from any supplier of telecommunication service or from any lawful authority the existence or place of origin or of destination of any telecommunication in order to obtain telecommunication service by fraud in violation of THIS subsection ~~A of this section~~.

4. Knowingly sells, rents, lends, gives, or otherwise transfers or discloses or attempts to transfer or disclose to another, or offers or advertises for sale or rental, any:

(a) SOFTWARE, instrument, apparatus, equipment or device described in paragraph 3 of this subsection~~; or~~.

(b) Plans, specifications or instructions for making or assembling ~~the same~~ ANY SOFTWARE, INSTRUMENT, APPARATUS, EQUIPMENT OR DEVICE with the intent to use or employ such SOFTWARE, instrument, apparatus, equipment or device, or any part ~~thereof,~~ OF ANY SOFTWARE, INSTRUMENT, APPARATUS, EQUIPMENT OR DEVICE or to allow ~~the same~~ ANY SOFTWARE, INSTRUMENT, APPARATUS, EQUIPMENT OR DEVICE to be used or employed, for a purpose described in paragraph 3 of this subsection~~, or that the~~.

(c) Plans, specifications or instructions ~~are intended to~~ WITH THE INTENT THAT THE PLANS, SPECIFICATIONS OR INSTRUCTIONS be used for making or assembling such SOFTWARE, instrument, apparatus, equipment or device, or any part ~~thereof~~ OF ANY SOFTWARE, INSTRUMENT, APPARATUS, EQUIPMENT OR DEVICE.

B. Subsection A, paragraph 3 of this section does not prohibit the use or possession of any SOFTWARE, instrument, apparatus, equipment or device by either of the following:

1. Law enforcement officers who are acting in their official capacity within the scope of their authority and in the line of duty.

2. Employees or agents of communication service providers as defined in section ~~13-3004~~ 13-3001 who are acting in their official capacity within the scope of their employment for the purpose of protecting the property or legal rights of the provider.

C. THIS SECTION APPLIES WHEN THE TELECOMMUNICATION SERVICE ORIGINATES OR TERMINATES OR BOTH ORIGINATES AND TERMINATES IN THIS STATE.

~~C.~~ D. ~~Telecommunications~~ TELECOMMUNICATION fraud is a class 3 felony.

~~D.~~ E. As used in this section:

~~1. "Telecommunication services" includes telephone and telegraph services and all other services involving the transmission of information by wire, radio, cellular, wireless transmission or similar means. This section applies when the telecommunication service originates or terminates or both originates and terminates in this state.~~

~~2.~~ 1. "Credit card number" means the card number appearing on a credit card, ~~or~~ telephone calling card ~~which~~ OR ACCESS DEVICE AS DEFINED IN SECTION 13-2001 THAT is ~~an identification card or plate~~ issued to a person by any supplier of telecommunication service and ~~which~~ THAT permits the person to whom the card OR ACCESS DEVICE has been issued to obtain telecommunication service.

2. "TELECOMMUNICATION SERVICE" INCLUDES ELECTRONIC COMMUNICATION SERVICES, SUBSCRIPTION COMPUTER SERVICES, TELEPHONE AND TELEGRAPH SERVICES AND ALL OTHER SERVICES THAT INVOLVE THE TRANSMISSION OF INFORMATION BY WIRE, RADIO, CELLULAR, WIRELESS TRANSMISSION OR SIMILAR MEANS.

Sec. 33. Section 13-4801, Arizona Revised Statutes, is amended to read:

13-4801. Definitions

In this chapter, unless the context otherwise requires:

1. "Acquire" means to electronically capture, record, reveal or otherwise access by means of any instrument, device or equipment a cellular or wireless telephone's electronic serial number or mobile identification number without the consent of the communication service provider.

2. "Cellular telephone" means a communication device that contains an electronic serial number and the operation of which depends on the transmission of that electronic serial number together with the mobile identification number in the form of radio signals through cell sites and mobile switching stations.

3. "Cloned cellular or wireless telephone" means a cellular or wireless telephone in which the manufacturer's electronic serial number has been altered.

4. "Cloning paraphernalia" means the materials that are necessary to create a cloned cellular or wireless telephone and includes scanners to intercept electronic serial numbers, cellular telephones and mobile identification numbers, wireless telephones, cables, chips, burners, software and the computers containing the software to program a cloned cellular or wireless telephone's microchip with a false electronic serial number and mobile identification number combination and lists of electronic serial number and mobile identification number combinations.

5. "Communication service provider" has the same meaning prescribed in section ~~13-3004~~ 13-3001.

6. "Electronic serial number" means the unique numerical algorithm that the manufacturer programs into the microchip of each wireless telephone.

7. "Mobile identification number" means the cellular or wireless telephone number that the cellular or wireless telephone carrier assigns to the wireless telephone.

8. "Wireless telephone" means a communication device that transmits radio, satellite or other mobile telephone communication.

Sec. 34. Section 21-422, Arizona Revised Statutes, is amended to read:

21-422. Powers and duties

A. The law applicable to county grand juries, including their powers, duties and functions, ~~shall apply~~ APPLIES to the state grand juries except insofar as it is in conflict with this article. The ~~Arizona~~ supreme court shall ~~promulgate~~ ADOPT rules ~~and regulations~~ to govern the procedures of state grand juries.

B. The state grand jury shall investigate and return indictments for only those offenses or violations of law ARISING OUT OF OR IN CONNECTION WITH:

1. ~~Arising out of or in connection with~~ The determination or collection of state taxes, the registration or failure to register securities, the offer or sale of securities, the offer or sale of interests in land, the formation or operation of banks, insurance companies, pension funds, labor unions, professional sports enterprises, corporate enterprises, or business enterprises, the making or collecting of loans, events leading to receivership or declaration of bankruptcy by a business enterprise, the sale or purchase of goods or services by or for the state or political subdivisions, bribery, obstruction of justice, hindering prosecution or any form of intentional, knowing or corrupt misconduct involving any person compensated by public funds. ~~; or~~

2. ~~Arising out of or in connection with~~ Any fraud, theft or possession, receipt, sale or transportation of stolen property or other contraband, or gambling or prostitution or narcotics, which occurs in more than one county or which occurs in one county and affects the residents of another county or which may be prosecuted by more than one county attorney. ~~; or~~

3. ~~Arising out of or in connection with~~ Perjury, false swearing, unsworn falsification, or any violation of title 13, chapter 28 in connection with any state grand jury proceeding, committed by any person testifying before it or in any trial or other proceeding involving any indictment returned by a state grand jury. ~~; or~~

4. ~~Arising out of or in connection with~~ Any perjury by subornation or attempted perjury by subornation relating to testimony before it or in any trial or other proceeding involving any indictment returned by a state grand jury. ~~; or~~

5. ~~Arising out of or in connection with~~ Any violation of title 13, chapter 23 or section 38-421 or 39-161.

6. ANY VIOLATION OF TITLE 13, CHAPTER 35.1 IF COMMITTED USING A COMPUTER OR NETWORK AS DEFINED IN SECTION 13-2301 AND IF ANY PART OF THE CONDUCT EITHER:

(a) OCCURS IN MORE THAN ONE COUNTY, STATE OR COUNTRY.

(b) AFFECTS THE RESIDENTS OF ANOTHER COUNTY, STATE OR COUNTRY.

(c) MAY BE PROSECUTED BY MORE THAN ONE COUNTY, STATE OR COUNTRY.

7. ANY CRIMINAL WRONGDOING THAT IS REFERRED IN WRITING BY A COUNTY ATTORNEY AND THAT IS ACCEPTED IN WRITING BY THE ATTORNEY GENERAL.

C. If a state grand jury, pursuant to an investigation under subsection B of this section, learns of an offense for which it lacks jurisdiction to indict, the grand jury shall direct the attorney general to inform the appropriate prosecutorial authority.

D. Nothing in this article shall be construed to limit the jurisdiction of the county grand juries or county attorneys, nor shall an

investigation by a state grand jury be deemed preemptive of a previously instituted investigation by another grand jury or agency having jurisdiction under the same subject matter unless good cause is shown.

Sec. 35. Section 31-281, Arizona Revised Statutes, is amended to read:

31-281. Deoxyribonucleic acid identification; sexual offenses

A. A person WHO IS convicted of or adjudicated delinquent for a sexual offense or attempt to commit a sexual offense as provided in section 13-1403, 13-1404, 13-1405, 13-1406, 13-1410, 13-1411, 13-1412, 13-1417 or 13-3608 or WHO IS convicted of or adjudicated delinquent for a violation of section 13-3821, 13-3822, ~~or~~ 13-3824, 13-3552, 13-3553 OR 13-3554 and any person who is accepted under the interstate compact for the supervision of parolees and probationers and has arrived in this state shall submit to deoxyribonucleic acid testing for law enforcement identification purposes. THE DEPARTMENT OF PUBLIC SAFETY SHALL MAINTAIN reports of the tests ~~shall be maintained by the department of public safety~~.

B. A person who is tested pursuant to subsection A of this section and who has sufficient financial ability shall pay for the costs of the testing. The cost to the person shall not exceed five hundred dollars. All monies received pursuant to this subsection shall be transmitted to the state treasurer for deposit in the Arizona deoxyribonucleic acid identification system fund established by section 41-2419.

C. IF A JUVENILE IS ADJUDICATED DELINQUENT AND IS TESTED PURSUANT TO SUBSECTION A OF THIS SECTION, THE results of ~~any tests secured pursuant to this section from a person adjudicated delinquent~~ THE TEST may be used for any law enforcement identification purpose, including adult prosecutions.

Sec. 36. Section 44-405, Arizona Revised Statutes, is amended to read:

44-405. Preservation of secrecy; definition

A. In an action under this chapter OR SECTION 13-1802 OR 13-2316.02 a court shall preserve the secrecy of an alleged trade secret by reasonable means~~, which may include~~.

B. FOR THE PURPOSES OF THIS SECTION, "REASONABLE MEANS" INCLUDES granting protective orders in connection with discovery proceedings, holding in camera hearings, sealing the records of the action or ordering a person involved in the litigation not to disclose an alleged trade secret without prior court approval.

Sec. 37. Severability

If a provision of this act or its application to any person or circumstances is held invalid, the invalidity does not affect other provisions or applications of the act that can be given effect without the invalid provision or application, and to this end the provisions of this act are severable.

APPROVED BY THE GOVERNOR APRIL 7, 2000

FILED IN THE OFFICE OF THE SECRETARY OF STATE APRIL 7, 2000

Attorney General Janet Napolitano's Computer Crimes Act of 2000

Attorney General's Website

THE FIGHT TO KEEP THE INTERNET A SAFE PLACE FOR ARIZONA STUDENTS

Attorney General's Office Working to Protect Kids From Predators

The Internet is fast becoming a valuable source of educational and research material for students. As more and more classrooms are wired to the Information Superhighway, more and more students are becoming familiar and comfortable with the Internet as an educational tool.

Unfortunately, the Internet can also be a dangerous place for children. The threats posed by sites that promote sex, drugs, alcohol and other illegal activity are great. Attorney General Janet Napolitano is educating the public and fighting cyber-crime by utilizing several methods; for example:

EDUCATING PARENTS

In order to protect their children, parents today need to be educated about the Internet. Parents should know how they can ensure their children reap the educational benefits on being online without the exposure to potentially harmful material. In the first of a series of community town hall meetings Attorney General Napolitano and other community leaders conducted a briefing and provided material to help guide parents through this difficult issue. Pointing parents to Internet sites like www.getnetwise.com, where parents can learn about the risks their children face online, read about filtering products, and learn how to report trouble, is just one way to provide parents with the resources they need to keep their children safe.

EDUCATING LAW ENFORCEMENT

By adding a Technology Crimes Special Counsel to the Criminal Division of the Arizona Attorney General's Office the opportunity for urban and rural police departments and prosecutors to receive timely training about cyber- crime became available. The Office has been involved in conducting training around the State to help law enforcement identify, investigate, and prosecute computer crime effectively. In order to ensure our children are safe from online predators, we must make sure all law enforcement agencies are aware and informed on the latest laws and court decisions concerning computer crime.

PROSECUTING CYBER-CRIMINALS

"We intend to vigorously investigate and prosecute cyber-crime because of the intense threat it poses to our families and our children," said Attorney General Napolitano.

The Attorney General's Office has succeeded in taking several computer criminals offline. One recent case involved a man trying to steal money from banks using a complex computer network. He is now serving a one-year term in jail and seven years probation. In June the Attorney General indicted an Ohio man for conspiracy and sexual exploitation of a minor in an Internet sting operation. The Unit, led by a nationwide expert in the field of computer crime, is using state of the art methods to stop cyber-criminals before they strike again. Arizona is taking a proactive role in pulling criminals off the Internet, where they can harm children and defraud innocent citizens, and putting them behind bars.

SAFE SURFING: WAYS TO PROTECT YOUR CHILDREN

Tips for Parents and Families

- Locate your computer in a central, communal area of the house, such as the family room or den.
- Establish specific "Internet time" and stick to it.
- Call your child's school and inquire about the "acceptable use policy" for Internet use at school. Make sure you get a copy for your reference.
- If your child's school does not have such a policy, ask the school board to adopt one.
- Explain to your children that some sites on the Internet can be dangerous. Tell them if they ever see, hear, or read something that makes them uncomfortable, tell a parent immediately.
- Teach them direct ways to access information through kid-friendly search engines such as AOL NetFind Kids Only (http://www.aol.com/netfind/kids/home.html) or KidsClick! Web Search (http://www.sunsite.berkeley.edu/KidsClick!).
- Talk to your children regularly about their experiences on the Internet and what they have learned.
- Use the "Staying Safe Online: A Young Person's Contract" below.

STAYING SAFE ONLINE: A YOUNG PERSON'S CONTRACT

1. I will **ALWAYS** tell a parent or another adult immediately if something is confusing or seems scary or threatening.
2. I will **NEVER** give out my full name, real address, telephone number, school name, location, schedule, password, or other identifying information while I'm online. I will tell an adult anytime I am asked for that information.
3. I will **NEVER** have a face-to-face meeting with anyone I've met online without discussing the meeting with a parent or another adult and taking an adult with me.
4. I will **NEVER** respond online to any messages that use bad words or words that are scary, threatening, or make me feel uncomfortable. If I get that kind of message, I will print it and tell an adult immediately.
5. I will **NEVER** go into a new online area that is going to cost additional money without first asking permission from a parent or a teacher.
6. I will **NEVER** send a picture of myself, my friends, or my family to anyone unless I have my parent's permission.
7. I will **NEVER** give out a credit card number online without my parent present.

Parent_____ Young Person_____

Source: Parent's Guide to the Information Superhighway

Attorney General Janet Napolitano's Computer Crimes Act of 2000

News Articles

Arizona targeting cybercrime

Will introduce sweeping bill

By Robbie Sherwood
The Arizona Republic

State Attorney General Janet Napolitano is looking to turn Arizona into the nation's leader in ferreting out and stopping cybercrime with a sweeping bill in the upcoming legislative session.

The Computer Crime Act of 2000 would outlaw the creation of destructive and annoying computer viruses, stalking via the Internet and the growing problem of "screen jacking," where Web sites, often pornographic, override a computer's exit function and won't let the computer user rid the screen of an offensive image.

The proposed legislation also defines a new crime: "luring." It would be a felony to solicit children online by transmitting sexually explicit material to them or to a school, Napolitano said.

"If passed, it will be the best and most comprehensive cybercrime package in the nation," she said.

California has the most comprehensive set of cybercrime laws, but Arizona's would be more practical, the attorney general said. Arizona's bill outlines computer crimes in general descriptive terms. California's law refers to specific technologies, requiring a retooling of the legislation each time a new technology is developed, "which occurs about every hour," Napolitano said.

— *Please see* **ARIZONA**, *Page A8*

> *"If passed, it will be the best and most comprehensive cybercrime package in the nation.*
>
> **JANET NAPOLITANO**
> ARIZONA ATTORNEY GENERAL

INTERNET ARREST: Tempe man sought teen for sex, police say. **A29.**

Republic, A1
12.9.99

Arizona is aiming to curb cybercrime

ARIZONA, *from Page A1*

Sen. Marc Spitzer, R-Phoenix, and Rep. John Verkamp, R-Flagstaff, have sponsored the bill, which is now being circulated to drum up more support.

"I think it has a very good chance to make it through the Legislature," Verkamp said of the bill. "We need to update all of our statutes to take in the High Technology Age. A lot of them are kind of antiquated."

For example, there is little in Arizona law to deal with online stalkers. Napolitano said a young man, angry at his girlfriend, recently posted pictures of her on the Internet and sent out sexually explicit e-mail under her assumed identity. The young man had essentially invited others to do his stalking for him. The new law would change that, Napolitano said.

"You won't be able to avoid the stalking statutes even if you didn't actually do the stalking. If you just set it up," she said. "If you start putting stuff on the Internet, you have exponentially expanded the audience, and the danger to the victim, in my view."

Robbie Sherwood can be reached at robbie.sherwood@arizonarepublic.com or at (602) 444-7938.

Republic, 12.9.99

A8 THE TRIBUNE. THURSDAY. DECEMBER 9. 1999 EV

AG targets 'cyberstalking,' kiddie porn, seeks new laws

BY HOWARD FISCHER
CAPITOL MEDIA SERVICES

Attorney General Janet Napolitano wants sweeping new laws to crack down on Internet crimes ranging from computer hacking to distributing kiddie porn.

Napolitano said the state's laws have not kept pace with technology and Internet growth. The result, she said, is some people are getting away with fraud, stalking and criminal mischief because laws don't address those crimes.

Even when an existing law can be applied, Napolitano said prosecution can be difficult. She also said the punishment may not fit the crime.

Her main target is making some computer hacking a Class 2 felony — a charge normally applied to cases such as manslaughter, or sex with minors.

Napolitano

Napolitano said that hacking — breaking into a computer through telephone lines — is not just idle amusement.

Last year, she said someone broke into the Salt River Project's billing database to cancel another person's account. Once inside, the hacker accessed computers that control the Valley's irrigation canal system.

Napolitano also wants to create a crime of "cyberstalking."

She said existing anti-stalking laws require some sort of physical contact between the perpetrator and victim. On the Internet, that contact may never take place.

Other types of computer harassment also need laws, Napolitano said.

Earlier this year, a young man who was angry at his former girlfriend posted pictures and assumed her identity on the Internet. He then used her identity to trade sexually explicit e-mail with others and put the woman in danger by inviting people to her home and office.

Napolitano said there also are gaps in child pornography laws.

She wants to protect repair technicians and others who report finding child pornography on a computer. Another change would make it illegal to "lure" a child online with the intent of sexual exploitation.

Also in Daily Star

Internet criminals, beware

That was some kind of long weekend Randy Parsons enjoyed back in January 1998. Thursday through Tuesday, he said, with a lot of drinking. A weekend like that can blow millions of brain cells.

Maybe that's why, during that long weekend, he logged on to the Internet and pretended to be someone else. Who he pretended to be was his ex-girlfriend, Tammy Farris, who had just broken off their relationship (hmm, we wonder why).

While pretending to be Ms. Farris, he sent out graphic messages inviting total strangers to come see her for sex. He posted her phone number, her workplace and directions to her home.

In a moral world this would have elicited no response whatsoever. But like roaches crawling out of the sewer in search of the latest morsel, dozens of people followed up by calling Ms. Farris. Some even showed up at her home after midnight. That none of them were homicidal maniacs was a blessing. She could have wound up dead.

To the degree that cyberspace has provided a new home for criminals and perverts, it has posed a new challenge for law enforcement. In many ways it's a challenge that affects Americans' fundamental bedrock freedoms as protected in the First and Fourth Amendments to the Constitution. There's a lot of law yet to be made in this realm.

Fortunately, the Arizona Attorney General's Office has tried to stay on top of the game by creating a new Technology Crimes Unit. This unit eventually tracked down Parsons and threw the book at him. He pleaded guilty last month to felonious theft of identity and last week he was sentenced to spend 30 days in jail.

He also was ordered to avoid unsupervised use of the Internet for three years. On top of that, he will be required to undergo psychosexual evaluation to determine whether he should be registered as a sex offender (the vote in this corner is yes on that), and he may receive mandatory counseling as well for "Internet addiction." Without such counseling, it is feared, Parsons might repeat his award-winning performance in cyberfiction.

Parsons himself told *The Tribune* that's unlikely. He wrote the whole thing off to that long, lost weekend and said it wouldn't happen again. All in all, he's happy with the sentence.

Farris isn't. She'd like to have seen her ex-beau tossed in the clink for the whole 2½ years the law allows for such crimes. She's right. That's what should have happened.

But to the degree that it sobers up Mr. Parsons and puts other such would-be felons on notice that cybercrime is no game, it's a step in the right direction.

We have entered an amazing new age with the Internet. It's a marvelous research tool and communications device. But since human nature is imbued with a sometimes domineering dark side, we probably have only begun to learn how it can be misused to the detriment of others. Law enforcement is going to have to strive mightily to keep up.

We're fortunate that the Arizona Attorney General's Office is trying.

Tribune 10.25.99

New laws needed to deal with cybercriminals

MY TURN

JANET NAPOLITANO

As we transition into a new century and new millennium, it's time we look at how some of the advances in technology have had an impact on our society. While computers have become incredibly beneficial to us, there are some individuals who use these remarkable machines to do harm. As such, we must now reform our laws to allow us to go after the few who wield computers as weapons to commit crimes.

While we have been able to prosecute some computer crimes using our current statutes, there are instances in which these offenses may go unpunished, mainly because our computer-crime laws have not kept pace with technology.

Arizona's computer-crimes statute was drafted in 1978, in the days of eight-track music players and the 15-cent first class postage stamp. That was also about the time that Bill Gates was dropping out of college, before anyone had heard of e-mail, Windows, Apple Computer or banking by phone.

Who would have ever dreamed that between then and now, a home computer device would become so advanced? That we would be able to have interactive mail discussions with people on the other side of the equator or listen to radio stations that broadcast from across the globe? Or that we could gather research and access information on almost any topic known to humans within seconds, using the Internet? It's time we update our laws to reflect these changes.

As quickly as technology advances, so does the criminal element. The Internet, which is opening a whole new world to businesses and consumers, is also a playground for con artists, pedophiles, hatemongers and sociopaths. That is why this month, I have sent to the state Legislature the Computer Crimes Act of 2000, the most comprehensive "cybercrime" bill in the country.

My office is working with a bipartisan group of lawmakers, including House Speaker Jeff Groscost, Sen. Marc Spitzer, Sen. Chris Cummiskey, Rep. John Loredo, Sen. Joe Eddie Lopez and Rep. John Verkamp, to amend our criminal code to specify some computer crimes and beef up the penalties for crimes committed with the use of a computer.

Soliciting sex from children is by no means a new crime. But Internet chat rooms and electronic mail provide pedophiles a new way to go after their prey, all without ever leaving home and often in the middle of nowhere using a laptop computer. Because this type of communication is so unique, we need to specifically criminalize the act of using the Internet to lure a child for sex or offering a child for the purpose of sexual exploitation.

Additionally, the Computer Crimes Act of 2000 would make it a felony for someone to intentionally send sexually explicit material to a child and would protect computer repair technicians or others who report such crimes.

"Cyberstalking" has become a real problem. Last year, my office prosecuted the first case of its kind in Arizona, in which a young woman was "stalked" by strangers because her disgruntled former boyfriend thought he would play a prank by posing as the woman on the Internet and sending out sexually explicit e-mails. This prompted strangers to visit and call her at all hours of the day and night at work, home and school.

The victim didn't own a computer, hadn't talked with nor seen the perpetrator in months, yet found her life completely disrupted by him. Under the Computer Crimes Act of 2000, this criminal behavior would be prosecuted for what it is. No perpetrator would be able to hide behind a computer as an excuse for committing this crime.

Computers have become a real asset for businesses to store customer information, business records and financial data and use as a communication and research tool. Our proposal would put teeth in existing statutes meant to prevent criminals from sabotaging companies' databases and bringing business to a standstill. It would also add specific actions to the list of crimes that occur in this area.

Other vital components of the Computer Crimes Act of 2000 include imposing stiffer penalties for individuals who use high-tech means to upset important systems such as water, emergency services, utilities, traffic control, etc.; protecting businesses from theft of trade secrets, identity theft, credit card fraud, forgery and other acts; and bringing law enforcement's ability to preserve time-sensitive electronic evidence into the 21st century.

The time for changes to our computer-crime laws is ripe. I believe that the Computer Crimes Act of 2000, which was carefully written to protect our citizens and punish criminals, is at least for now the most comprehensive in the country to inhibit computer crime.

Janet Napolitano is attorney general of Arizona. Readers are invited to submit columns of up to 625 words.

Arizona Republic
January 25, 2000

Funds sought to battle state Internet crime

Lawmaker's plan backed by Napolitano

By Howard Fischer
Capitol Media Services

PHOENIX – A key House member wants $500,000 to help the state fight crime on the Internet.

"When you're looking at e-crime, this is the future," said Rep. Jim Weiers, R-Phoenix. "It's no different than being held up in a Circle K parking lot with a gun."

Weiers, who is the House majority whip, said yesterday that the government has a legitimate role in protecting its citizens from becoming victims of the latest kind of crime. Lawmakers, he said, should be willing to provide the resources.

The idea secured endorsement from George Weisz, the governor's top aide for law enforcement and criminal justice. Weisz, a former assistant attorney general, said funding is needed to ensure the state has the equipment to track down people making e-mail threats and promoting hate on the Internet.

But that doesn't translate to cash: The proposed $500,000 won't be part of the budget Gov. Jane Hull presents next month to the Legislature.

"Obviously it's a worthy cause," Hull said, but noted that the budget was put together long before her office was ever informed of Weiers' plan.

Even if that weren't the case, Hull said she still may not support the plan because it could divert resources from other pet projects.

"The question is, do we not fund behavioral health (programs) again? Do we not fund education?" she asked. "Where do we cut?"

Attorney General Janet Napolitano, who is working with Weiers on his plan, said the additional funds for fighting Internet crime should be a priority.

She said the the state should approach the computer-related "crime scene" in the same manner it deals with crime in other settings.

Napolitano said one of the most pervasive problems her office contends with is adults using the Internet as a method of luring children into meetings in which the concealed purpose is to pursue sexual contact.

"Kids are taught not to talk to strangers," she said. "But that doesn't translate on the Net" with youngsters more willing to share information with others who could be who they say they are – or could be someone else.

Napolitano said her office now operates "stings," in which investigators pose as young girls sending online messages to see who tries to lure them. But, she said, her agency needs upgraded equipment and resources for tracing messages to their source.

Daily Star
12-21-99

Wednesday, December 29, 1999
Paradise Valley, Arizona
THE TOWN OF PARADISE
VALLEY INDEPENDENT
Page: 4

AG offers tips to protect children from Internet, computer dangers

Computers are bringing an enormous amount of new information into our homes and many children are going on-line to explore cyberspace. While much of what they can access by logging onto the Internet is educational and fun, there is also a potential for unsafe and exploitative situations. The Internet is a global "network of networks" and is not regulated by any government entity. This means there are very few limits or checks on the kinds of information that is provided by and accessible to Internet users.

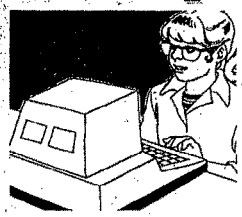
Parents can minimize the risk their children might encounter on-line by keeping the following safety tips in mind:

• Participate in your children's computer use. Explore the Internet with them, get to know the services they use and learn how to log onto these yourself.

• Log children onto the Internet provider yourself and keep the password secret. If you allow older children to have their own passwords, know what these are and instruct your kids to never share a password with anyone else.

• Set a family rule that no one should ever give out personally identifying information, such as last name, home address, telephone number, age, school name or address to anyone you meet in a public forum like a chat room or a bulletin board. Children need to understand that it's easy for people to misrepresent themselves and their real identifies on-line.

• Chat rooms are probably the most dangerous area on the Internet because they can be used by adults to initiate sexual contact with children. For this reason, children should never give our personal information or share anything on-line that they would not want to appear in public. Teach children to log off and tell you immediately if they get or encounter any scary or sexually oriented information.



• Children should never arrange an in-person meeting with someone they meet on-line without your permission and involvement. If you agree to such a meeting, have it in a public location and be sure to accompany your child.

• Share your children's e-mail accounts and if they receive any material in a message or bulletin board that is frightening or harassing, forward a copy to your on-line service provider and ask for their assistance. An on-line service provider can exercise some limited control over the materials that its subscribers distribute, but remember the Internet as a whole is not regulated.

• In general, it's best to not respond to an e-mail from someone you don't know. By responding, you are verifying your e-mail address and that information can be used by a person who might send more inappropriate e-mails or put you on a list.

• Possessing and distributing child pornography is illegal. If anyone in your family receives such materials, report it to your service provider, to the National Center for Missing and Exploited Children's CyberTipline at 1-800-843-5678, and to your local law enforcement agency.

• Check out filtering programs that block objective materials.

These "parent controls" are available from your service provider or as special software you can buy. Filters work in various ways — some block Web sites, some prevent users from entering certain kinds of information like name and address, while others restrict your children's ability to enter certain chat rooms. Unfortunately, no filter can completely protect your child, so parental supervision is essential. Several blocking and monitoring products are available via Web site at www.getnetwise.org.

Janet Napolitano
Attorney General

EDITORIALS

New era demands new law

Arizona Attorney General Janet Napolitano is right in urging the Legislature to create a new law to crack down on the spread of Internet-based crime.

Quite simply, the state's criminal code has not kept pace with the rapid migration of human misconduct into cyberspace.

Current anti-stalking laws, for example, require physical contact between the stalker and the stalked before a prosecution may be initiated.

That lets stalkers sending intimidating e-mail get away. Likewise, relatively gentle laws regulate "hacking" into others' computer systems via phone lines, which, in fact, can create grave public danger if it disrupts massive regional electric, water or communications grids.

Napolitano, given that, would smartly do three things: She would create new law to cover new offenses; she would make the punishment for some "cybercrimes" fit their real seriousness; and she would make certain prosecutions – now difficult – a little easier.

A new crime of "cyberstalking" needs designation to cover online harassment that may never involve the face-to-face contact required by existing stalking laws. The same goes for "luring" – the heinous use of the Internet to solicit or offer children for sexual exploitation.

Dozens of such cases are being worked right now in Arizona, but their legal standing can be nebulous. Napolitano would change that with her Computer Crime Act of 2000. And she would appropriately add special categories to tighten up also on online credit card and identity fraud and computer disruption.

Regarding punishments, meanwhile, it also seems right to establish harsher penalties for certain forms of computer hacking, for instance.

Take the incident last year when a hacker cracked into a billing database of the Salt River Project in Phoenix looking to cancel an account. Far from merely making mischief, that hacker also managed to gain access to the computers that control SRP's entire irrigation control system – a potentially major intrusion.

Surely the Legislature should accede to Napolitano's proposal that such serious forms of hacking be promoted from Class 6 or Class 4 felonies to Class 2, on a par with manslaughter. Hacking's disruption can be that serious.

Finally, it makes no sense that the state, when tracking the source of improper messages, should have to obtain a warrant to inspect each and every computer system the message passed through. Consider that a hacker's data connection that paralyzes a business' in-house computer system may run through six different Internet servers or more. Shouldn't a single warrant to trace the hacker's path suffice? Of course it should.

But then, so it goes with virtually all of the attorney general's cybercrime package. The world has changed, and so have the means of misbehavior. By recognizing that, Napolitano's bill performs the necessary service of bringing the law to the Internet. The Legislature should pass it.

Daily Star 12.15.99

Senator KYL. Thank you very much. That is very helpful, and I have got several questions that I have noted.

But let me first turn to our next witness, Mr. Guadalupe Gonzalez, the special agent in charge of the FBI's Phoenix Field Office. Mr. Gonzalez has served in his post since August 1998. Prior to coming to Phoenix, he was the special agent in charge of organized crime, drugs, and violent crimes in the FBI's Los Angeles office.

Mr. Gonzalez, thank you very much for testifying at today's hearing. As I noted before, your full written statement will be placed in the record. I would like to invite you to make any summary remarks at this time, and I would note to the people who are here, in the hearing that we held a couple of weeks ago in Washington, DC, on this same subject, the FBI Director Louis Freeh presented his testimony, and in asking him how best to relate that testimony to people in Arizona, he suggested that we ask Mr. Gonzalez to be his representative here. And we are delighted to do that, so thank you.

STATEMENT OF GUADALUPE GONZALEZ

Mr. GONZALEZ. Good morning, Mr. Chairman. Thank you for inviting me to the field hearing to discuss the growing problem of cyber crime and our response to it. Our ability in the field to deal with this crime problem requires the support of Congress. The recent denial-of-service attacks against Yahoo, Amazon.com, eBay, CNN, Buy.com, and other e-commerce websites have thrust the security of our information infrastructure into the spotlight. But they are only one example of a large and growing problem of criminal activity in cyberspace. I would like to discuss with you the national challenge of battling computer intrusions.

The cyber revolution has permeated virtually every facet of our lives, and we see its effects all around us in the way we communicate, do business, and even in the way Government operates. Unfortunately, that revolution has affected the nature of criminal activity as well. Criminals are increasingly seeing the utility of cyber tools to facilitate traditional crimes such as fraud, extortion, and dissemination of child pornography. And they are also inventing new forms of crime which make computers and the information stored on them the targets of the crime. Thus, we see criminals intruding into computers to steal credit card numbers, to abscond with proprietary information, and to shut down e-commerce sites. And this is not just a criminal problem. It is also a national security problem. This is because our Nation's critical infrastructures, by which I mean those services that are vital to our economy and national security, such as electrical energy, telecommunications, banking and finance, transportation, and government operations, are now dependent on computer technology for their very operations. And this very dependence makes them vulnerable to an attack which, if successful, could deny service on a broad scale.

The same basic types of cyber attack tools, therefore, become attractive not only to criminals interested in illicit financial gain, but also to foreign intelligence services seeking new ways to obtain sensitive government or industry information and to terrorists of hostile foreign nations bent on attacking U.S. interests.

The difficulty of dealing with this challenge stems from the nature of the cyber environment. The cyber environment is borderless, afford easy anonymity and methods of concealment to bad actors, and provides new tools to allow for remote access to targeted computers. A criminal sitting on the other side of the planet is now capable of stealthily infiltrating a computer network in Arizona to steal money, abscond with proprietary information, or shut down e-commerce sites.

To deal with this problem, law enforcement has retooled its workforce, its equipment, and its own information infrastructure. It must also forge new partnerships with private industry, other agencies, and our international counterparts.

We at the FBI have been doing all of these things for the last 2 years, but we must continue to build upon our progress to ensure that we can perform our responsibilities to protect public safety and national security in the information age.

My written statement provides an overview of the broad spectrum of cyber threats which gives a flavor of the incredibly varied nature of the threats we face. The examples range from insiders bent on revenge against their employers, to hackers seeking bragging rights in the hacking community, to criminal groups stealing credit card numbers or money, to foreign intelligence agencies or foreign military services who target U.S. interests.

The most common threats we face are from hackers and criminals stealing for profit. For example, in March, authorities in the United Kingdom, acting in coordination with the FBI, arrested two individuals for alleged intrusions into e-commerce sites in several countries and the theft of credit card information on over 26,000 accounts. One subject used the Internet alias "CURADOR." Losses from this case could exceed $3 million. The FBI cooperated closely with the Dyfed–Powys Police Department in the United Kingdom and the Royal Canadian Mounted Police in Canada and private industry.

Here in Arizona, we are investigating a computer intrusion case in which a private enterprise was defrauded of several hundred thousand dollars in fraudulent telephone calls that were placed to a foreign country.

We are also concerned about the terrorist threat. Terrorist groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely. Director of Central Intelligence George Tenet has testified that terrorist groups, "including Hizbollah, Hamas, the Abu Nidal organization, and Bin Laden's al Qa'ida organization are using computerized files, e-mail, and encryption to support their operations."

While we have not yet seen these groups employ cyber tools as a weapon to use against critical infrastructures, their reliance on information technology and acquisition of computer expertise are clear warning signs.

Finally, given the presence of military research facilities in Arizona, we must be concerned with national security threats. As you know, the FBI has observed a series of intrusions into numerous Department of Defense and other Federal Government computer networks and private sector entities. An investigation last year de-

termined that the intrusions appear to have originated in Russia. The intruder successfully accessed U.S. Government networks and took large amounts of unclassified but sensitive information, including defense technical research information.

Here in Arizona, we have seen scans of military computer systems by outside intruders. Some of the logs indicate that the source of some of these scans may be foreign.

The recent distributed denial-of-service attacks have garnered a tremendous amount of interest in the public. Because the FBI is actively investigating these attacks, I cannot provide a detailed briefing on the status of our efforts. However, I can tell you that all FBI field offices, including the Phoenix Division, have been asked to assist on a case to the extent that entities in our jurisdiction are involved in the matter or to the extent that we can cover leads within our jurisdiction.

In February 1998, the National Infrastructure Protection Center, NIPC, was established as a focal point for the Federal Government's efforts to protect the critical infrastructures. On October 2, 1998, the center was designated a branch of the FBI's National Security Division, and the National Infrastructure Protection and Computer Intrusion Program was approved as an investigative program. This program is a tier one priority under the FBI's strategic plan and serves as the FBI's vehicle for performing the infrastructure protection mission assigned to the NIPC under Presidential Decision Directive 63. In October 1999, the program was moved to a newly-formed Counterterrorism Division of the FBI, reflecting the FBI's high priority on protecting the infrastructures from terrorist threats.

At headquarters, the NIPC has a budget of approximately $21 million. This is not slated to increase in fiscal year 2001. There are currently 193 agents in the field devoted to NIPC matters as well as 101 personnel at FBI headquarters. The NIPC at headquarters also houses 19 interagency detailees, mainly from the law enforcement, defense, and intelligence communities. The NIPC works closely with foreign counterparts on case-related matters.

Beyond the NIPC at FBI headquarters, a cyber crime investigative program has been created in all FBI field offices, including the Phoenix Division. We have special agents here who are responsible for investigating computer intrusions, viruses, or denial-of-service attacks, and for conducting critical liaison activities with private industry. Given the amount of work we have and the fact that Phoenix is the sixth largest city in the United States, we are seeking to establish a full computer intrusion squad in the Phoenix Division by the year 2002.

One major difficulty that distinguishes cyber threats from physical threats is determining who is attacking your system, why, how, and from where. This difficulty stems from the ease with which individuals can hide or disguise their tracks by manipulating logs and directing their attacks through networks in many countries before hitting their ultimate target. This will continue to pose a problem as long as the Internet remains rife with vulnerabilities and allows easy anonymity and concealment.

Another significant challenge we face is intrusions involving multiple jurisdictions. A typical investigation involves victim sites in

multiple States and often many countries. This is the case even when the hacker and the victim are both located in the United States. In the United States, we can subpoena records, engage in judicially approved electronic surveillance, and execute search warrants on suspects' homes, seize evidence, and examine it. We can do none of these things ourselves overseas; rather, we depend on the local authorities to assist us.

The most difficult situation will arise, however, when a foreign country with interests adverse to our own simply refuses to cooperate. In such a situation, we could find that an investigation is stymied unless we can find an alternative method of tracing the activity back to its source.

Our challenge lies in continuing to expand our computer investigative, analytic, training, and outreach programs. Given the explosive and continued growth of computer intrusions, the Infrastructure Protection and Computer Intrusion Program needs to more than double the current number of field investigative personnel and headquarters analysts. In addition, we need to leverage our resources by expanding our training programs to reach more State, local, and international investigators. Finally, NIPC investigators need high-speed computer processing and large-capacity storage for investigations.

I have tried to review with you some of the threats and challenges we face. Some of the challenges stem from the structure of the present loss governing computer crime. For example, we should ask whether the sentencing guidelines for computer crime are adequate and whether the $5,000 threshold for damage is a useful benchmark, because in many cases the true damage cannot be measured in monetary terms. Examples of damage difficult to measure monetarily are impairment of medical diagnosis, threat to public safety, or damage to national security, national defense, or administration-of-justice computers.

Another problem we face is having to obtain multiple trap and trace orders for different jurisdictions. The Kyl-Schumer bill addresses these concerns and other concerns. We support the goal of Senate bill 2092 to strengthen the general deterrence aspects of the Computer Fraud and Abuse Act and to provide some needed procedural enhancements to help us confront the expanding criminal threat in this dynamic and important part of our national economy, while continuing to protect individual privacy interests. The FBI looks forward to working with this committee on this important legislation.

Addressing the threat of cyber crime requires teamwork—teamwork among Government agencies, teamwork between Federal, State, and local law enforcement, and teamwork between the Government and the private sector. We have made much progress in establishing this sort of teamwork on all three fronts over the last 2 years. The FBI is also developing cyber crime task forces in partnership with State and local law enforcement entities within their jurisdiction to leverage the limited resources in this area. The first one was founded in Pittsburgh in March. We hope that one can be established in our jurisdiction in the next few years as the program expands.

The partnerships we have established with the private sector are particularly important for several reasons. Most of the victims of cyber crimes are private companies; therefore, successful investigation and prosecution of cyber crimes depends on private victims reporting incidents to law enforcement and cooperating with investigators. Second, the network administrator, who alone knows the intricacies of his or her network, often must provide critical assistance to the investigation leading him to the evidence of the intruder's activity.

Much has been said over the last few years about the importance of information sharing. Here in the Phoenix Division, we have an excellent working relationship with our private sector counterparts and the community in general. We share information on a number of areas, including infrastructure protection, and receive information from the private sector that greatly assists in protecting the community.

As a result of our close working relationship with the private sector, we can detect criminal activity in its initial stages and in some cases prevent criminal incidents. The NIPC also provides the private sector with warning information which also lessens their vulnerability. These warnings assist field offices like Phoenix to be better prepared and better protect our community. They further allow us the opportunity to respond quickly and efficiently to cyber threats. I believe that as companies continue to gain experience in dealing with the NIPC and the FBI field offices, as we continue to provide them with important and useful threat information, and as companies recognize that cyber crime requires a joint effort by industry and Government together, we will continue to make real progress in the area.

Our Key Asset Initiative facilitates response to threats and intrusion incidents by building liaison and communication links with the owners and operators of individual companies in the critical infrastructure sectors and enabling contingency planning. The Key Asset Initiative initially will involve determining which assets are key within the jurisdiction of each FBI field office and obtaining 24-hour points of contact at each asset in cases of emergency. Eventually, if future resources permit, the initiative will include the development of contingency plans to respond to attacks on each asset, exercises to test response plans, and modeling to determine the effects of an attack on particular assets.

Here in the Phoenix Division, we have identified dozens of key assets around the State for including in the national list. These assets include power generation facilities, water storage and distribution centers, transportation assets, military installations, research institutions, and key public emergency service entities.

The second is the InfraGard initiative. This is an initiative that we have developed in concert with private companies and academia to encourage information sharing about cyber intrusions, exploited vulnerabilities, and physical infrastructure threats. A vital component of InfraGard is the ability of industry to provide information on intrusions to the local FBI field offices using secure e-mail communications in both a sanitized and detailed format. We can use the detailed version to initiate an investigation, while NIPC headquarters can analyze that information in conjunction with other in-

formation we obtain to determine if the intrusion is part of a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company.

Here in Phoenix, we are planning to roll out our InfraGard Chapter on May 9. We expect to have representatives from in-state universities, businesses, and some of the critical infrastructures on hand.

We look forward to working with Congress to ensure that law enforcement can continue to address the cyber crime problem in the year ahead.

Thank you.

[The prepared statement of Mr. Gonzalez follows:]

PREPARED STATEMENT OF GUADALUPE GONZALEZ

INTRODUCTION

Mr. Chairman, Members of the Subcommittee: Thank you for inviting me to discuss the threats to our Nation's critical infrastructures and the FBI's approach in the field to meeting those challenges. In February 1998 the National Infrastructure Protection Center (NIPC) was established as a focal point for the federal government's efforts to protect the critical infrastructures. Following the founding of the Center, the National Infrastructure Protection and Computer Intrusion Program (NIPCIP) was approved as an FBI investigative program. NIPCIP is a Tier One priority under the FBI Strategic Plan and serves as the FBI vehicle for performing the NIPC's missions under PDD–63. In October 1999 the NIPCIP was moved to the newly-formed Counterterrorism Division of the FBI, reflecting the FBI's high priority on protecting the infrastructures from terrorist threats.

With the support of Congress and in particular the leadership of this committee, the NIPCI program has rapidly developed in FBI field offices across the United States, including here in Arizona. Today I will focus on the nature of the national security and criminal threats we face in cyberspace, the progress we have made in meeting those threats in the field, and the continuing challenges we face.

THE NIPC

The NIPC is an interagency Center located at the FBI. Created in 1998, the NIPC serves as the focal point for the government's efforts to warn of and respond to cyber attacks, particularly those that are directed at our nation's "critical infrastructures." These infrastructures include telecommunications and information, energy, banking and finance, transportation, government operations, and emergency services. Presidential Decision Directive (PDD) 63 directed that the NIPC serve as a "national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity." The PDD further states that the mission of the NIPC "will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response."

In field offices such as Phoenix, we have created a cyber crime investigative program called the National Infrastructure Protection and Computer Intrusion (NIPCI) Program. This program, managed by the NIPC, consists of special agents in each FBI Field Office who are responsible for investigating computer intrusions, viruses, or denial of service attacks, for implementing our key asset initiative, and for conducting critical liaison activities with private industry. Cyber crime task forces are being developed in partnership with state and local law enforcement entities within their jurisdiction to leverage the limited resources in this area. The first one opened in Pittsburgh last month.

THE BROAD SPECTRUM OF THREATS

Cybercrime threats faced by law enforcement

Before discussing the FBI's programs and requirements with respect to cybercrime, let me take a few minutes to discuss the dimensions of the problem. The FBI's case load is increasing dramatically. In fiscal year 1998, it opened 547 computer intrusion cases; in fiscal year 1999, that had jumped to 1,154. At the same time, because of the opening the National Infrastructure Protection Center (NIPC) in February 1998, and improving ability to fight cyber crime, more cases were

closed. In fiscal year 1998, 399 intrusion cases were closed, and in fiscal year 1999, 912 such cases were closed. However, given the exponential increase in the number of cases opened, cited above, the actual number of pending cases has increased by 39 percent, from 601 at the end of fiscal year 1998, to 834 at the end of fiscal year 1999. In short, even though the FBI has markedly improved its capabilities to fight cyber intrusions, the problem is growing even faster.

A few days ago the Computer Security Institute released its fifth annual "Computer Crime and Security Survey." The results only confirm what we had already suspected given our burgeoning case load, that more companies surveyed are reporting intrusions, that dollar losses are increasing, that insiders remain a serious threat, and that more companies are doing more business on the Internet than ever before.

The statistics tell the story. Ninety percent of respondents detected security breaches over the last 12 months. At least 74 percent of respondents reported security breaches including theft of proprietary information, financial fraud, system penetration by outsiders, data or network sabotage, or denial of service attacks. Information theft and financial fraud caused the most severe financial losses, put at $68 million and $56 million respectively. The losses from 273 respondents totaled just over $265 million. Losses traced to denial of service attacks were only $77,000 in 1998, and by 1999 had risen to just $116,250. Further, the new survey reports on numbers taken before the high-profile February attacks against Yahoo, Amazon and eBay. Finally, many companies are experiencing multiple attacks; 19 percent of respondents reported 10 or more incidents.

Over the past several years the FBI has seen a range of computer crimes from defacement of websites by juveniles to sophisticated intrusions that we suspect may be sponsored by foreign powers, and everything in between. Some of these are obviously more significant than others. The theft of national security information from a government agency or the interruption of electrical power to a major metropolitan area have greater consequences for national security, public safety, and the economy than the defacement of a web-site. But even the less serious categories have real consequences and, ultimately, can undermine confidence in e-commerce and violate privacy or property rights. A website hack that shuts down an e-commerce site can have disastrous consequences for a business. An intrusion that results in the theft of credit card numbers from an online vendor can result in significant financial loss and, more broadly, reduce consumers' willingness to engage in e-commerce. Because of these implications, it is critical that we have in place the programs and resources to investigate and, ultimately, to deter these sorts of crimes.

The following are some of the categories of cyber threats that we confront today.

Insiders. The disgruntled insider (a current or former employee of a company) is a principal source of computer crimes for many companies. Insiders' knowledge of the target companies' network often allows them to gain unrestricted access to cause damage to the system or to steal proprietary data. The just-released 2000 survey by the Computer Security Institute and FBI reports that 71 percent of respondents detected unauthorized access to systems by insiders.

In January and February 1999 the National Library of Medicine (NLM) computer system, relied on by hundreds of thousands of doctors and medical professionals from around the world for the latest information on diseases, treatments, drugs, and dosage units, suffered a series of intrusions where system administrator passwords were obtained, hundreds of files were downloaded which included sensitive medical "alert" files and programming files that kept the system running properly. The intrusions were a significant threat to public safety and resulted in a monetary loss in excess of $25,000. FBI investigation identified the intruder as Montgomery Johns Gray, III, a former computer programmer for NLM, whose access to the computer system had been revoked. Gray was able to access the system through a "backdoor" he had created in the programming code. Due to the threat to public safety, a search warrant was executed for Gray's computers and Gray was arrested by the FBI within a few days of the intrusions. Subsequent examination of the seized computers disclosed evidence of the intrusion as well as images of child pornography. Gray was convicted by a jury in December 1999 on three counts for violation of Title 18 U.S.C. § 1030. Subsequently, Gray pleaded guilty to receiving obscene images through the Internet, in violation of 47 U.S.C. 223.

Hackers. Hackers (or "crackers") are also a common threat. They sometimes crack into networks simply for the thrill of the challenge or for bragging rights in the hacker community. Recently, however, we have seen more cases of hacking for illicit financial gain or other malicious purposes.

While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus while attack tools have become

more sophisticated, they have also become easier to use. The distributed denial-of-service (DDOS) attacks last month are only the most recent illustration of the economic disruption that can be caused by tools now readily available on the Internet.

Another recent case illustrates the scope of the problem. In March, authorities in the United Kingdom, acting in coordination with the FBI, arrested two individuals for alleged intrusions into e-commerce sites in several countries and the theft of credit card information on over 26,000 accounts. One subject used the Internet alias "CURADOR." Losses from this case could exceed $3,000,000. The FBI cooperated closely with the Dyfed-Powys Police Service in the United Kingdom, the Royal Canadian Mounted Police in Canada, and private industry. This investigation involved the Philadelphia Division, seven other FBI field offices, our Legal Attache in London, and the NIPC. This case demonstrates the close partnerships that we have built with our foreign law enforcement counterparts and with private industry.

We are making some progress in convicting hackers. For example, on March 8, 2000, FBI Boston Division and New Hampshire Police arrested Dennis M. Moran, aka COOLIO, in association with the unauthorized intrusion and changes made to the Drug Abuse Resistance Education's (DARE) Web site, violating New Hampshire State Laws 638: 17 and 638: 18(I), unauthorized access into a computer system, unauthorized changes to a computer system and damage to a computer system exceeding $1,000.00. It is anticipated that the New Hampshire State Attorney's Office will prosecute Moran, who is 17, as an adult. The United States Attorney's Office for the District of New Hampshire has therefore deferred prosecution of Moran to the State.

In April, Patrick Gregory, the co-founder of the hacker group known as "Global Hell," was convicted of a single count of conspiracy to commit telecommunications wire fraud and computer hacking in Texas U.S. District Court. He currently awaits sentencing.

Virus Writers. Virus writers are posing an increasingly serious threat to networks and systems worldwide. Last year saw the proliferation of several destructive computer viruses or "worms," including the Melissa Macro Virus, the Explore.Zip worm, and the CIH (Chernobyl) Virus. The NIPC frequently sends out warnings or advisories regarding particularly dangerous viruses, which can allow potential victims to take protective steps and minimize the destructive consequences of a virus.

The Melissa Macro Virus was a good example of the NIPC's two-fold response—encompassing both warning and investigation—to a virus spreading in the networks. The NIPC sent out warnings as soon as it had solid information on the virus and its effects; these warnings helped alert the public and reduce the potential destructive impact of the virus. On the investigative side, the NIPC acted as a central point of contact for the field offices who worked leads on the case. A tip received by the New Jersey State Police from America Online, and their follow-up investigation with the FBI's Newark Division, led to the April 1, 1999 arrest of David L. Smith. Mr. Smith pleaded guilty to one count of violating 18 U.S.C. § 1030 in Federal Court, and to four state felony counts. As part of his guilty plea, Smith stipulated to affecting one million computer systems and causing $80 million in damage. Smith is awaiting sentencing.

Criminal Groups. We are also seeing the increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain. In September, 1999, two members of a group dubbed the "Phonemasters" were sentenced after their conviction for theft and possession of unauthorized access devices (18 USC § 1029) and unauthorized access to a federal interest computer (18 USC § 1030). The "Phonemasters" were an international group of criminals who penetrated the computer systems of MCI, Sprint, AT&T, Equifax, and even the National Crime Information Center. Under judicially approved electronic surveillance orders, the FBI's Dallas Division made use of new technology in the investigation. One suspect, Mr. Calvin Cantrell, downloaded thousands of Sprint calling card numbers, which he sold to a Canadian individual, who passed them on to someone in Ohio. These numbers made their way to an individual in Switzerland and eventually ended up in the hands of organized crime groups in Italy. Cantrell was sentenced to two years as a result of his guilty plea, while one of his associates, Cory Lindsay, was sentenced to 41 months.

The Phonemasters' methods included "dumpster diving" to gather old phone books and technical manuals for systems. They used this information to trick employees into giving up their logon and password information. The group then used this information to break into victim systems. It is important to remember that often "cyber crimes" are facilitated by old fashioned guile, such as calling employees and tricking them into giving up passwords. Good cyber security practices must therefore address personnel security and "social engineering" in addition to instituting electronic security measures.

Beyond criminal threats in cyber space, we also face a variety of significant national security threats

Terrorists. Terrorists groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely. In his statement on the worldwide threat in 2000, Director of Central Intelligence George Tenet testified that terrorists groups, "including Hizbollah, HAMAS, the Abu Nidal organization, and Bin Laden's al Qa'ida organization are using computerized files, e-mail, and encryption to support their operations." In one example, convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his laptop computer. While we have not yet seen these groups employ cyber tools as a weapon to use against critical infrastructures, their reliance on information technology and acquisition of computer expertise are clear warning signs. Moreover, we have seen other terrorist groups, such as the Internet Black Tigers (who are reportedly affiliated with the Tamil Tigers), engage in attacks on foreign government websites and e-mail servers. "Cyber terrorism"—by which I mean the use of cyber tools to shut down critical national infrastructures (such as energy, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population—is thus a very real, though still largely potential, threat.

Foreign intelligence services. Not surprisingly, foreign intelligence services have adapted to using cyber tools as part of their espionage tradecraft. Even as far back as 1986, before the worldwide surge in Internet use, the KGB employed West German hackers to access Department of Defense systems in the well-known "Cuckoo's Egg" case. Foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. Government and private sector information.

More recently, we observed a series of intrusions into numerous Department of Defense and other federal government computer networks and private sector entities. Investigation last year determined that the intrusions appear to have originated in Russia. The intruder successfully accessed U.S. Government networks and took large amounts of unclassified but sensitive information, including defense technical research information. The NIPC coordinated a multi-agency investigation, working closely with FBI field offices, the Department of Defense, and the Intelligence Community.

Information Warfare. The prospect of "information warfare" by foreign militaries against our critical infrastructures is perhaps the greatest potential cyber threat to our national security. We know that several foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States or other nations. Knowing that they cannot match our military might with conventional or "kinetic" weapons, some nations see cyber attacks on our critical infrastructures or military operations as a way to hit what they perceive as America's Achilles heel—our growing dependence on information technology in government and commercial operations. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. And a Russian official has also commented that an attack on a national infrastructure could, "by virtue of its catastrophic consequences, completely overlap with the use of [weapons] of mass destruction."

Distributed denial of service tools

The recent distributed denial of service (DDOS) attacks on e-commerce sites have garnered a tremendous amount of interest in the public and in the Congress. While we do not yet have official damage estimates, the Yankee Group, a research firm, estimates the impact of the attacks at $1.2 billion due to lost capitalization losses, lost revenues, and security upgrades. Because we are actively investigating these attacks, I cannot provide a detailed briefing on the status of our efforts. However, I can provide an overview of our activities to deal with the DDOS threat beginning last year and of our investigative efforts. These attacks illustrate the growing availability of destructive, yet easy-to-use, exploits that are widely available on the Internet. They also demonstrate the NIPC's two-fold mission: sharing information with the private sector and warning of possible threats, and responding to actual attacks.

In the fall of last year, the NIPC began receiving reports about a new set of "exploits" or attack tools collectively called distributed denial of service (or DDOS) tools. DDOS variants include tools known as "Trin00," "Tribal Flood Net" (TFN), "TFN2K," and "Stacheldraht" (German for "barbed wire"). These tools essentially work as follows: hackers gain unauthorized access to a computer system(s) and place software code on it that renders that system a "master" (or a "handler"). The hackers also intrude into other networks and place malicious code which makes

those systems into agents (also known as "zombies" or "daemons" or "slaves"). Each Master is capable of controlling multiple agents. In both cases, the network owners normally are not aware that dangerous tools have been placed and reside on their systems, thus becoming third-party victims to the intended crime.

The "Masters" are activated either remotely or by internal programming (such as a command to begin an attack at a prescribed time) and are used to send information to the agents, activating their DDOS ability. The agents then generate numerous requests to connect with the attack's ultimate target(s), typically using a fictitious or "spoofed" IP (Internet Protocol) address, thus providing a falsified identity as to the source of the request. The agents act in unison to generate a high volume of traffic from several sources. This type of attack is referred to as a SYN flood, as the SYN is the initial effort by the sending computer to make a connection with the destination computer. Due to the volume of SYN requests the destination computer becomes overwhelmed in its efforts to acknowledge and complete a transaction with the sending computers, degrading or denying its ability to complete service with legitimate customers—hence the term "Denial of Service". These attacks are especially damaging when they are coordinated from multiple sites—hence the term Distributed Denial of Service.

An analogy would be if someone launched an automated program to have hundreds of phone calls placed to the Capitol switchboard at the same time. All of the good efforts of the staff would be overcome. Many callers would receive busy signals due to the high volume of telephone traffic.

In November and December, the NIPC received reports that universities and others were detecting the presence of hundreds of agents on their networks. The number of agents detected clearly could have been only a small subset of the total number of agents actually deployed. In addition, we were concerned that some malicious actors might choose to launch a DDOS attack around New Year's Eve in order to cause disruption and gain notoriety due to the great deal of attention that was being paid to the Y2K rollover. Accordingly, we decided to issue a series of alerts in December to government agencies, industry, and the public about the DDOS threat.

Moreover, in late December, it was determined that a detection tool that was developed by the NIPC for investigative purposes might also be used by network operators to detect the presence of DDOS agents or masters on their operating systems, and thus would enable them to remove an agent or master and prevent the network from being unwittingly utilized in a DDOS attack. Moreover, at that time there was, to our knowledge, no similar detection tool available commercially. The NIPC therefore decided to take the unusual step of releasing the tool to the Department of Defense, other government agencies, and to the public in an effort to reduce the level of the threat. The first variant of our software was made available on the NIPC web site on December 30, 1999. To maximize the public awareness of this tool, we announced its availability in an FBI press release that same date. Since the first posting of the tool, we have posted three updated versions that have perfected the software and made it applicable to different operating systems.

The public has downloaded these tools tens of thousands of times from the web site, and has responded by reporting many installations of the DDOS software, thereby preventing their networks from being used in attacks and leading to the opening of criminal investigations both before and after the widely publicized attacks of the last few weeks. The work with private companies has been so well received that the trade group SANS awarded their yearly Security Technology Leadership Award to members of the NIPC's Special Technologies Applications Unit.

In February, reports were received that a new variation of DDOS tools was being found on Windows operating systems. One victim entity provided us with the object code to the tool found on its network. On February 18 the binaries were made available to anti-virus companies (through an industry association) and the Computer Emergency Response Team (CERT) at Carnegie Mellon University for analysis and so that commercial vendors could create or adjust their products to detect the new DDOS variant. Given the attention that DDOS tools have received in recent weeks, there are now numerous detection and security products to address this threat, so it was determined that the NIPC could be most helpful by giving them the necessary code rather than deploying a detection tool ourselves.

Unfortunately, the warnings that we and others in the security community had issued about DDOS tools last year, while alerting many potential victims and reducing the threat, did not eliminate the threat. Quite frequently, even when a threat is known and patches or detection tools are available, network operators either remain unaware of the problem or fail to take necessary protective steps. In addition, in the cyber equivalent of an arms race, exploits evolve as hackers design variations to evade or overcome detection software and filters. Even security-conscious companies that put in place all available security measures therefore are not invulnerable.

And, particularly with DDOS tools, one organization might be the victim of a successful attack despite its best efforts, because another organization failed to take steps to keep itself from being made the unwitting participant in an attack.

On February 7, 2000, the NIPC received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship that we have developed with the private sector, in the days that followed, several other companies (including Cable News Network, eBay, Amazon.com, Buy.com, and ZDNET), also reported denial of service outages to the NIPC or FBI field offices. These companies cooperated with us by providing critical logs and other information. Still, the challenges to apprehending the suspects are substantial. In many cases, the attackers used "spoofed" IP addresses, meaning that the address that appeared on the target's log was not the true address of the system that sent the messages. In addition, many victims do not keep complete network logs.

The resources required in an investigation of this type are substantial. Companies have been victimized or used as "hop sites" in numerous places across the country, meaning that we must deploy special agents nationwide to work leads. We currently have seven FBI field offices with cases opened and all the remaining offices are supporting the offices that have opened cases. Agents from these offices are following up literally hundreds of leads. The NIPC is coordinating the nationwide investigative effort, performing technical analysis of logs from victims sites and Internet Service Providers (ISP's), and providing all-source analytical assistance to field offices. Moreover, parts of the evidentiary trail have led overseas, requiring us to work with our foreign counterparts in several countries through our Legal Attaches (Legats) in U.S. embassies. Here in Phoenix we followed up on leads resulting from the DDOS attacks.

While the crime may be high tech, investigating it involves a substantial amount of traditional investigative work as well as highly technical work. Interviews of network operators and confidential sources can provide very useful information, which leads to still more interviews and leads to follow-up. And victim sites and ISP's provide an enormous amount of log information that needs to be processed and analyzed by human analysts.

CHALLENGES IN COMBATING CYBER INTRUSIONS

The burgeoning problem of cyber intrusions, viruses, and denial of service attacks poses unique challenges to the NIPC. These challenges require novel solutions, close teamwork among agencies and with the private sector, and adequate human and technical resources.

Identifying the Intruder. One major difficulty that distinguishes cyber threats from physical threats is determining who is attacking your system, why, how, and from where. This difficulty stems from the ease with which individuals can hide or disguise their tracks by manipulating logs and directing their attacks through networks in many countries before hitting their ultimate target. The "Solar Sunrise" case illustrates this point. This will continue to pose a problem as long as the Internet remains rife with vulnerabilities and allows easy anonymity and concealment.

Jurisdictional Issues. Another significant challenge we face is intrusions involving multiple jurisdictions. A typical investigation involves victim sites in multiple states and often many countries. This is the case even when the hacker and victim are both located in the United States. In the United States, we can subpoena records, engage in judicially approved electronic surveillance, and execute search warrants on suspects' homes, seize evidence, and examine it. We can do none of those things ourselves overseas; rather, we depend on the local authorities to assist us. However, some local police forces do not have the technical resources or expertise to provide assistance. In other cases, these nations may not have laws against computer intrusions and are therefore limited in their ability to help us. FBI Legal Attaches in 35 embassies abroad provide critical help in building bridges with local law enforcement to enhance cooperation on cyber crime and in working leads on investigations. As the Internet spreads to even more countries, we will see greater demands placed on the Legats to support computer crime investigations. The NIPC also has held international computer crime conferences and offered cyber crime training classes to foreign law enforcement officials to develop liaison contacts and bring these officials up to speed on cyber crime issues.

The most difficult situation will arise, however, in which a foreign country with interests adverse to our own simply refuses to cooperate. In such a situation, we could find that an investigation is stymied unless we find an alternative method of tracing the activity back to its source.

THE LEGAL LANDSCAPE

To deal with this crime problem, we must look at whether changes to the legal procedures governing investigation and prosecution of cyber crimes are warranted. The problem of Internet crime has grown at such a rapid pace that the laws have not kept up with the technology. The FBI is working with the Department of Justice to propose a legislative package for your review to help keep our laws in step with these advances.

One example of some of the problems law enforcement is facing is the jurisdictional limitation of pen registers and trap-and-trace orders issued by federal district courts. These orders allow only the capturing of tracing information, not the content of communications. Currently, in order to track back a hacking episode in which a single communication is purposely routed through a number of Internet Service Providers that are located in different states, we generally have to get multiple court orders. This is because, under current law, a federal court can order communications carriers only within its district to provide tracing information to law enforcement. As a result of the fact that investigators typically have to apply for numerous court orders to trace a single communication, there is a needless waste of time and resources, and a number of important investigations are either hampered or derailed entirely in those instances where law enforcement gets to a communications carrier after that carrier has already discarded the necessary information. For example, Kevin Mitnick evaded attempts to trace his calls by moving around the country and by using cellular phones, which routed calls through multiple carriers on their way to the final destination. It was impossible to get orders quickly enough in all the jurisdictions to trace the calls.

Finally, we should consider whether current sentencing provisions for computer crimes provide an adequate deterrence. Given the degree of harm that can be caused by a virus, intrusion, or a denial of service—in terms of monetary loss to business and consumers, infringement of privacy, or threats to public safety when critical infrastructures are affected—it would be appropriate to consider, as S. 2092 does, whether penalties established years ago remain adequate.

Evaluation of the effectiveness of 18 U.S.C. § 1030 and the tools to enforce it under both current law and under S. 2092.—Generally, 18 U.S.C. § 1030 has enabled the FBI and other law enforcement agencies to investigate and prosecute persons who would use the power of the Internet and computers for criminal purposes. Nonetheless, just as computer crime has evolved over the years, so too must our laws and procedures evolve to meet the changing nature of these crimes.

One persistent problem is the need under current law to demonstrate at least $5,000 in damage for certain hacking offenses enumerated by 18 U.S.C. § 1030(a)(5). In some of the cases investigated by the FBI, damages in excess of $5,000 on a particular system are difficult to prove. In other cases, the risk of harm to individuals or to the public safety posed by breaking into numerous systems and obtaining root access, with the ability to destroy the confidentiality or accuracy of crucial—perhaps lifesaving information—is very real and very serious even if provable monetary damages never approach the $5,000 mark. In investigations involving the dissemination or importation of a virus or other malicious code, the $5,000 threshold could potentially delay or hinder early intervention by Federal law enforcement.

S. 2092 significantly adjusts the $5,000 threshold and other provisions in the current law by: (1) creating a misdemeanor offense for those cases where damages are below $5,000, while simultaneously adjusting the minimum mandatory sentences under the Sentencing Guidelines; and (2) moving the aggravating factors previously included in the definition of"damage" under 18 U.S.C. § 1030(e)(8) (such as impairment of medical diagnosis, physical injury to any person, threat to public health or safety or damage to nation security, national defense or administration of justice computers) to the general sentencing provisions of § 1030(c) (where they will be on par in serious cases with the existing $5,000 threshold requirement and will expose offenders to an enhanced 10-year period of imprisonment up from the current maximum of 5 years). The critical element here is that the criminal intended to cause damage, not the specific amount of damage he intended to cause

Another issue involves the alarming number of computer hackers encountered in our investigations who are juveniles. Under current law, Federal authorities are not able to prosecute juveniles for any computer violations of 18 U.S.C. § 1030. S. 2092 would authorize (but not require) the Attorney General to certify for juvenile prosecution in Federal court youthful offenders who commit the more serious felony violations of section 1030. Recognizing that this change will, over time, result in the prosecution of repeat offenders, S. 2092 also defines the term "conviction" under § 1030 to include prior adjudications of juvenile delinquency for violations of that section. This is intended to provide greater specific deterrence to juveniles who are

adjudicated delinquent for computer hacking. Similarly, a majority of the States have enacted criminal statutes prohibiting unauthorized computer access analogous to the provisions of section 1030. As State prosecutions for these offenses increase, the likelihood of encountering computer offenders in Federal investigations who have prior State convictions will similarly rise. The Department is studying whether prior state adult convictions for comparable computer crimes justify enhanced penalties for violations of section 1030, just as prior State convictions for drug offenses trigger enhanced penalties for comparable Federal drug violations.

Law enforcement also needs updated tools to investigate, identify, apprehend and successfully prosecute computer offenders. Today's electronic crimes, which occur at the speed of light, cannot be effectively investigated with procedural devices forged in the last millennium during the infancy of the information technology age. Statutes need to be rendered technology neutral so that they can be applied regardless of whether a crime is committed with pen and paper, e-mail, telephone or geosynchronous orbit satellite personal communication devices.

As discussed above, a critical factor in the investigation of computer hacking cases is law enforcement's ability to swiftly identify the source and the direction of a hacker's communications. Like all law enforcement agencies, the FBI relies upon the pen register and trap and trace provisions contained in 18 U.S.C. § 3121 *et seq.* to seek court approval to acquire data identifying non-content information relating to a suspect's communications. Our ability to identify the perpetrators of crimes like computer hacking is directly proportional to our ability to quickly acquire the necessary court orders and quickly serve them upon one or more service providers in a communications chain. Under current law, however, valuable time is consumed in acquiring individual court orders in the name of each communications company for each newly discerned link in the communications chain even though the legal justification for the disclosure remains unchanged and undiminished. S. 2092 would amend 18 U.S.C. § 3123(a) to authorize Federal courts to issue one nation-wide order which may then be served upon one or more service providers thereby substantially reducing the time necessary to identify the complete pathway of a suspect's communication. Second, S. 2092 makes the statute more technology neutral by, among other things, inserting the terms "or other facility" wherever "telephone" appears. This change codifies Federal court decisions that apply the statute's provisions not merely to traditional telephone, but to an ever expanding array of other, communications facilities. Together, these are important changes that do not alter or lower the showing necessary for the issuance of the court order but which do enhance the order's usefulness to law enforcement.

We support the goal of S. 2092 to strengthen the general deterrence aspects of the Computer Fraud and Abuse Act, and to provide some needed procedural enhancements to help us confront the expanding criminal threat in this dynamic and important part of our national economy while continuing to protect individual privacy interests. The FBI looks forward to working with the Committee on this important legislation.

INTERAGENCY COOPERATION

The broad spectrum of cyber threats described earlier, ranging from hacking to foreign espionage and information warfare, requires not just new technologies and skills on the part of investigators, but new organizational constructs as well. In most cyber attacks, the identity, location, and objective of the perpetrator are not immediately apparent. Nor is the scope of his attack—i.e., whether an intrusion is isolated or part of a broader pattern affecting numerous targets. This means it is often impossible to determine at the outset if an intrusion is an act of cyber vandalism, organized crime, domestic or foreign terrorism, economic or traditional espionage, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to gather information from the victim sites and intermediate sites such as ISP's and telecommunications carriers. Under our constitutional system, such information typically can be gathered only pursuant to criminal investigative authorities. This is why the NIPC is part of the FBI, allowing us to utilize the FBI's legal authorities to gather and retain information and to act on it, consistent with constitutional and statutory requirements.

But the dimension and varied nature of the threats also means that this is an issue that concerns not just the FBI and law enforcement agencies, but also the Department of Defense, the Intelligence Community, and civilian agencies with infrastructure-focused responsibility such as the Departments of Energy and Transportation. It also is a matter that greatly affects state and local law enforcement. This is why the NIPC is an interagency center, with representatives detailed to the FBI from numerous federal agencies and representation from state and local law enforce-

ment as well. These representatives operate under the direction and authority of the FBI, but bring with them expertise and skills from their respective home agencies that enable better coordination and cooperation among all relevant agencies, consistent with applicable laws.

In Phoenix, we work closely with the U.S. military as well as other government agencies. For example, we have worked with U.S. military installations located in Arizona on attempted intrusions into their systems. The expansion of cyber task forces, such as the one just started in Pittsburgh, to other field divisions such as Phoenix, should assist us with interagency cooperation.

PRIVATE SECTOR COOPERATION

Our success in battling cyber crime also depends on close cooperation with private industry. This is the case for several reasons. First, most of the victims of cyber crimes are private companies. Therefore, successful investigation and prosecution of cyber crimes depends on private victims reporting incidents to law enforcement and cooperating with the investigators. Contrary to press statements by cyber security companies that private companies won't share information with law enforcement, many private companies have reported incidents and threats to the NIPC or FBI field offices. While there are undoubtedly companies that would prefer not to report a crime because of the subsequent loss of consumer confidence, the situation has improved markedly. Companies increasingly realize that deterrence of crime depends on effective law enforcement, and that the long-term interests of industry depend on establishing a good working relationship with government to prevent and investigate crime.

Second, the network administrator at a victim company or ISP is critical to the success of an investigation. Only that administrator knows the unique configuration of their system, and the administrator typically must work with an investigator to find critical transactional data that will yield evidence of a criminal's activity.

Third, the private sector has the technical expertise that is often critical to resolving an investigation. It would be impossible for us to retain experts in every possible operating system or network configuration, so private sector assistance is critical. In addition, many investigations require the development of unique technical tools to deal with novel problems. Private sector assistance has been critical there as well.

We have several other initiatives devoted to private sector outreach that bear mentioning here. The first is called "InfraGard." This is an initiative that we have developed in concert with private companies and academia to encourage information-sharing about cyber intrusions, exploited vulnerabilities, and physical infrastructure threats. A vital component of InfraGard is the ability of industry to provide information on intrusions to the local FBI field office using secure e-mail communications in both a "sanitized" and detailed format. The local FBI field offices can, if appropriate, use the detailed version to initiate an investigation; while NIPC Headquarters can analyze that information in conjunction with other information we obtain to determine if the intrusion is part of a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. The key to this system is that whether, and what, to report is entirely up to the reporting company. A secure web site also contains a variety of analytic and warning products that we make available to the InfraGard community. The success of InfraGard is premised on the notion that sharing is a two-way street: the NIPC will provide threat information that companies can use to protect their systems, while companies will provide incident information that can be used to initiate an investigation and to warn other companies.

Here in Phoenix, we are planning to roll-out our InfraGard Chapter on May 9. We expect to have representatives from in state universities, businesses, and some of the critical infrastructures on hand.

Our Key Asset Initiative (KAI) is focused more specifically on the owners and operators of critical components of each of the infrastructure sectors. It facilitates response to threats and incidents by building liaison and communication links with the owners and operators of individual companies and enabling contingency planning. The KAI began in the 1980's and focused on physical vulnerabilities to terrorism. Under the NIPC, the KAI has been reinvigorated and expanded to focus on cyber vulnerabilities as well. The KAI currently involves determining which assets are key within the jurisdiction of each FBI Field Office and obtaining 24-hour points of contact at each asset in cases of emergency. Eventually, if future resources permit, the initiative will include the development of contingency plans to respond to attacks on each asset, exercises to test response plans, and modeling to determine

the effects of an attack on particular assets. FBI field offices are responsible for developing a list of the assets within their respective jurisdictions, while the NIPC maintains the national database. The KAI is being developed in coordination with DOD and other agencies. Currently the database has about 2,600 entries. This represents 2,600 contacts with key private sector nodes made by the NIPC and FBI field offices.

Here in the Phoenix Division, we have identified dozens of key assets around the state for inclusion in the national list. These assets include power generation facilities, water storage and distribution centers, transportation assets, military installations, research institutions, and key public emergency service entities.

Much has been said over the last few years about the importance of information sharing. Here in the Phoenix Division, we have an excellent working relationship with our private sector counterparts and the community in general. We share information on a number of areas, including infrastructure protection, and receive information from the private sector that greatly assist us in protecting the community. As a result of our close working relationship with the private sector we can detect criminal activity in its initial stages and in some cases prevent criminal incidents. The NIPC also provides the private sector with warning information which also lessens their vulnerability. These warnings assist field offices like Phoenix to be better prepared and better protect our community. They further allow us the opportunity to respond quickly and efficiently to cyber threats. I believe that as companies continue to gain experience in dealing with the NIPC and FBI field offices, as we continue to provide them with important and useful threat information, and as companies recognize that cyber crime requires a joint effort by industry and government together, we will continue to make real progress in this area.

MEETING THE GROWING CYBER THREAT

As Internet use continues to soar, the number of cyber attacks is also increasing exponentially. Nationally there are over 1000 open computer intrusion cases. Further, this figure does not count computer facilitated crimes such as Internet fraud, child pornography, or e-mail extortion efforts. In these cases, the NIPC and NIPCI squads often provide technical assistance to traditional investigative programs responsible for these categories of crime.

We can clearly expect these upward trends to continue, and for the threats to become more serious. While insiders, hackers, and criminal groups make up much of our case load at the moment, we can anticipate a growing number of national security cases in the near future. To meet this challenge, we must ensure that we have adequate resources, including both personnel and equipment, both at the NIPC and in FBI field offices. We currently have 193 agents nationwide dedicated to investigating computer intrusion and virus cases. In order to maximize investigative resources the FBI has taken the approach of creating regional squads in 16 field offices that have sufficient size to work complex intrusion cases and to assist those field offices without a NIPCI squad. In those field offices without squads, the FBI is building a baseline capability by having one or two agents work NIPC matters, i.e. computer intrusions (criminal and national security), viruses, InfraGard, state and local liaison, etc.

The Phoenix office has a three agent team working on infrastructure protection and computer intrusion matters. Three agents are assigned to investigate cyber child pornography, and additional four agents are assigned to the Computer Assisted Response Team (CART), which is responsible to provide cyber forensics in support of all the cyber investigations in the Phoenix office. Since January 1, 2000 the Phoenix office has opened 9 new computer intrusion cases. This represents an almost 100 percent increase in computer intrusion cases opened in 1999.

Currently, at NIPC Headquarters, there are 101 personnel on board, including 82 FBI employees and 19 detailees from other government agencies. This cadre of investigators, computer scientists, and analysts perform the numerous and complex tasks outlined above, and provide critical coordination and support to field office investigations. As the crime problem grows, we need to make sure that we keep pace by bringing on board additional personnel, including from other agencies and the private sector.

In addition to putting in place the requisite number of agents, analysts, and computer scientists in the NIPC and in FBI field offices, we must fill those positions by recruiting and retaining personnel who have the appropriate technical, analytical, and investigative skills. This includes personnel who can read and analyze complex log files, perform all-source analysis to look for correlations between events or attack signatures and glean indications of a threat, develop technical tools to address the constantly changing technological environment, and conduct complex net-

work investigations. There is a very tight market for information technology professionals. The Federal Government needs to be able to recruit the very best people into its programs. Fortunately, we can offer exciting, cutting-edge work in this area and can offer agents, analysts, and computer scientists the opportunities to work on issues that no one else addresses, and to make a difference to our national security and public safety. In addition, Congress provided the FBI with a pilot program that exempts certain technical personnel from the Title V civil service rules, which allows us to pay more competitive salaries and recruit and retain top notch personnel. Unfortunately, this pilot is scheduled to expire in November unless extended

Training and continuing education are also critical, and we have made this a top priority at the NIPC. In fiscal year 1999, we trained 383 FBI and other-government-agency students in NIPC sponsored training classes on network investigations and infrastructure protection. The emphasis for 2000 is on continuing to train federal personnel while expanding training opportunities for state and local law enforcement personnel. During fiscal year 2000, we plan to train approximately 740 personnel from the FBI, other federal agencies, and state and local law enforcement.

Developing and deploying the best equipment in support of the mission is also very important. Not only do investigators and analysts need the best equipment to conduct investigations in the rapidly evolving cyber system but the NIPC must be on the cutting edge of cyber research and development. Conducting a network intrusion or denial-of-service investigation often requires analysis of voluminous amounts of data. For example, one network intrusion case involving an espionage matter currently being investigated has required the analysis of 17.5 Terabytes of data. To place this into perspective, the entire collection of the Library of Congress, if digitized, would comprise only 10 Terabytes. The Yahoo DDOS attack involved approximately 630 Gigabytes of data, which is equivalent to enough printed pages to fill 630 pickup trucks with paper. Technical analysis requires high capacity equipment to store, process, analyze, and display data. Again, as the crime problem grows, we must ensure that our technical capacity keeps pace. We are also working closely with other agencies to ensure that we leverage existing resources to the fullest extent possible.

THE ROLE OF LAW ENFORCEMENT

Finally, I would like to conclude by emphasizing two key points. The first is that our role in combating cyber crime is essentially two-fold: (1) preventing cyber attacks before they occur or limiting their scope by disseminating warnings and advisories about threats so that potential victims can protect themselves; and (2) responding to attacks that do occur by investigating and identifying the perpetrator. This is very much an operational role. Our role is not to determine what security measures private industry should take, or to ensure that companies or individuals take them. It is the responsibility of industry to ensure that appropriate security tools are made available and are implemented. We certainly can assist industry by alerting them to the actual threats that they need to be concerned about, and by providing information about the exploits that we are seeing criminals use. But network administrators, whether in the private sector or in government, are the first line of defense.

Second, in gathering information as part of our warning and response missions, we rigorously adhere to constitutional and statutory requirements. Our conduct is strictly limited by the Fourth Amendment, statutes such as Title III and ECPA, and the Attorney General Guidelines. These rules are founded first and foremost on the protection of privacy inherent in our constitutional system. Respect for privacy is thus a fundamental tenet in all of our activities.

CONCLUSION

I want to thank the subcommittee again for giving me the opportunity to testify here today. The cyber threat is real, multifarious, and growing. The FBI is moving aggressively to meet this challenge by training investigators and analysts to investigate computer intrusion cases, equipping them with the latest technology, developing our analytic capabilities and warning mechanisms to head off or mitigate attacks, and closely cooperating with the private sector. We have already made considerable progress in developing our capabilities to protect public safety and national security in the Information Age. I look forward to working with Congress to ensure that we continue to be able to meet the threat as it evolves and grows. Thank you.

Senator KYL. Thank you very much, Mr. Gonzalez.

Let me begin by asking both of you a question. Mr. Gonzalez, you mentioned the multiple trap and trace issue, and I would like to

ask both of you a question about that. For the benefit of those who aren't familiar with it, currently Federal law requires that law enforcement obtain a separate court order for trap and trace authority in each jurisdiction through which a cyber attack travels. Obviously, it is important for law enforcement to be able to quickly trace a source of an attack, as both witnesses have mentioned.

Could either of you give some examples of how investigations have been bogged down by the need to get this trap and trace authority in each jurisdiction and how the legislation that Senator Schumer and I have introduced, which would provide for national trap and trace authority, would resolve that issue? Mr. Gonzalez.

Mr. GONZALEZ. Yes, Sir. Well, in terms of the ability to obtain the national trap and trace orders, as you mentioned, timeliness is of the essence. And because of the different nature of how companies involved in information technology deal with their records and their record systems, some records are destroyed faster than others, it is imperative that we be able to get those orders in a timely fashion and be able to get out to the place where we need to deliver the orders to recoup the information.

If in the cases we mentioned—we talked about a case, for example, where the hacker's victims are in three different States and to get there we go through, say, multiple providers of either communications services or Internet technology services in different jurisdictions, we have to individually go to each one of those areas, provide the necessary information to get the court order. If we were able to do it at one time, it would save us a tremendous amount of time, and we could almost simultaneously be at all those different locations at one time and obtaining the information we need.

Senator KYL. Attorney General Napolitano.

Ms. NAPOLITANO. Yes, Senator, in response to your question, there is a very big need for a Federal hot pursuit statute in cyberspace, and the bill that you and Senator Schumer have put forward I think is going to be very, very valuable in that respect for many of the problems that Special Agent Gonzalez has mentioned.

Let me give you two examples of cases where we have gotten bogged down and have had to do an inordinate amount of work to get a result.

One is the very recent case in Scottsdale where a juvenile sent a threat via e-mail and basically shut down one of the middle schools in Scottsdale while the police department and the bomb dogs came out and looked to see whether there was anything to the threat. While that was going on, our office was tracking down and working with law enforcement to track down the source of the e-mail, and we were trying to do it very, very quickly both because of the school disruptions and because we didn't know whether it was a serious threat or not a serious threat.

To do that, we ultimately in the course of that investigation had to obtain separate court orders in both California and Virginia to identify the source of the e-mail. It would have been much better as a State if we had access to a Federal hot pursuit law that would have allowed us to get basically nationwide service of an order to track that source.

A second example is one you may be familiar with, and it involved hacking into a local utility company. That ultimately re-

quired the prosecutors to get orders in very many States all over the country to identify the source of the hacking into a utility company here.

So two concrete examples where we have been slowed down, have had to do a lot of extra work, and it illustrates the need for us to be able to speed up the process.

Senator KYL. And just to ensure that there is no invasion of privacy or inhibition of exercise of constitutional rights, would this nationwide trap and trace authority in any way diminish the constitutional rights of any of the entities from whom you are trying to obtain information?

Ms. NAPOLITANO. No, it would not. You would still have to comply with the fourth amendment.

Senator KYL. And the fourth amendment requirements would require that the law enforcement officials do what with respect to obtaining an order?

Ms. NAPOLITANO. In terms of getting a trap and trace order?

Senator KYL. Yes.

Ms. NAPOLITANO. You would still have to get an order issued by a court. The difference would be it would have nationwide application.

Senator KYL. So you would still have to prove the same kind of probable cause to a judge for the issuance of the warrant that would exist in any other situation?

Ms. NAPOLITANO. Yes. I assume the basic statutory and constitutional requirements for obtaining orders for traps and traces would apply. The difference would be that we wouldn't have to do it over and over again for basically the same search.

Senator KYL. Right. This is a good example, it seems to me, of the law needing to evolve with technology, or technology is going to get way ahead of law enforcement's ability to protect the citizens of the country.

Ms. NAPOLITANO. That is right, because even a delay of a few hours while you go to another courthouse in Virginia or California can be very critical in these kinds of cases.

Senator KYL. Now, I gather it would be safe to say, from what both of you have testified, that in Arizona you have seen a significant increase in the amount of cyber crime. Would that be fair, Mr. Gonzalez?

Mr. GONZALEZ. Yes, Sir. We have had a significant increase, in fact, specifically since the beginning of this year. Our caseload has increased probably 5 times, and we suspect it will continue to increase.

Senator KYL. One of the cases that I believe you alluded to in your prepared testimony but you didn't mention in your summary was a situation involving a very potentially dangerous situation with the dams in the State of Arizona. Could you describe that in just a little bit of detail?

Ms. NAPOLITANO. Yes. This is a case—I believe it happened in 1995. There is a typo in the testimony. But what happened in this instance was a computer user hacked his way into the billing database of the Salt River Project. He was looking to cancel someone's account. He then thereafter gained access, high-level access to the canal controlling system.

Now, when that crime occurred, we didn't have the bill I was describing to you, Senator. He was actually, I think, charged with a class III computer fraud felony. He subsequently provided a great deal of cooperation in some other cases, and so he pled down to a probation-eligible offense. And I believe, ironically, he is working in computer security in the private sector now, be that as it may.

Under the new law in Arizona, such hacking into a vital infrastructure, which is a defined term in the law, would be a class II felony. Under our statutory scheme, that is the next most serious offense to a first-degree murder.

Senator KYL. And when will this new law take effect?

Ms. NAPOLITANO. July 18.

Senator KYL. OK. Great.

Just a few more questions here. Are there any—I alluded to this in my opening statement, the possibility that there are legal impediments to the sharing of information, particularly by the private sector, with law enforcement. How would you characterize the cooperation between industry and law enforcement during the investigation of cyber crimes? And are there any disincentives that you are aware of that need to be removed for companies to come forward once they have experienced an attack? I will address that to both of you.

Mr. GONZALEZ. Well, Sir, I think the cooperation is good. It is getting better. There is a tendency sometimes on the part of the private sector to be a little hesitant, maybe, in say reporting either attempted intrusions or intrusions because of the fear of the impact that it may have on their status in the community where they are working. However, I think as part of the InfraGard program that we talked about where we are basically being able to—we are starting to form partnerships with the private sector to where they have an ability to anonymously join that program and provide us information that we can either use specifically with detail to initiate case or sanitize for NIPC to use to disseminate to other members of the program in terms of potential either attempted intrusions or intrusions. I think as we work more through that system and basically show and convince the industry that it is a viable system and it can only help in terms of deterring attempted intrusions and in the case of where the intrusions are successful prosecuting the offenders, I think as we develop more of a track record in that area the industry will be much more willing to continue and move forward with that cooperative effort.

Senator KYL. Now, some people in industry have expressed a concern that their computers could be confiscated or critical components of their operations could be brought down during the course of an investigation, which would essentially paralyze their ability to do business. What kind of assurance can you give them that this would not occur?

Mr. GONZALEZ. Actually, it would be almost the opposite. What we need from the industry is, first of all, if they have either an attempted intrusion or an intrusion, we need a timely notification almost immediately so that we can respond. And the other thing is we need their assistance in terms of whether it be their systems administrators or people from their companies or businesses that have the expertise in their systems to help us go through their sys-

tem and identify the information and the evidence that can either provide leads for us, investigative leads, or determine how the intrusion occurred.

We do not seize their computers. We will not seize their computers, and we do our best to be as unobtrusive in terms of affecting their business operations. But we need their help and assistance in doing that, one, in the timeliness of the reporting of the intrusions and, two, in the use of their technical expertise for their systems to get us through the investigative process.

Senator KYL. Now, another related concern is going public with information, and, General Napolitano, let me ask you as well as Mr. Gonzalez this. Let's say a classic bank fraud intrusion occurs, or, as you say, somebody hacks into the utility to cancel out their bill, but let's say it is a bank and there is a suggestion here that the bank is potentially exposed to lose hundreds of millions of dollars as a result of this intrusion. They discover that internally. They obviously don't want the evening news to carry the story: ABC Bank losing hundreds of millions of dollars to a hacker. That would suggest to their customers that it is not a safe place to keep their money and so on.

How can the law enforcement and prosecution authorities ensure that that won't happen and, therefore, provide a good incentive for people to cooperate with law enforcement as soon as possible to get the critical information to law enforcement so that the perpetrators can be brought to justice?

Ms. NAPOLITANO. Senator, that is a difficult question because we find it in a lot of different areas where entities that are actually the victims of crime are reluctant to report it because of likely media attention. And certainly you sometimes cannot control the media. I know this will come as a shock, but sometimes they find their own things of interest.

But a couple of very concrete things can be done to increase, I think, the security that a business can have in working with law enforcement. One is to make greater use of and have the ability to make greater use of sealing orders in court to protect things like trade secret information, proprietary, computer security information, and the like. After all, the long-term damage to an institution or a business is not the one-day news story. It is having the actual data put into the public domain that would enable someone else to commit a similar crime. The new bill in Arizona that I described actually has some express statutory provisions in that regard. I believe in terms of sealing trade secret information, Federal law already had a provision. Most States don't have something similar.

Senator KYL. Mr. Gonzalez, anything to add?

Mr. GONZALEZ. I would offer a couple of comments, Sir. In terms of publicity and public awareness, generally speaking, with the FBI and with the numerous Attorney General guidelines we have regarding the contacts with the media, information that is relayed to us or is reported to us a potential crime does not necessarily intimate that it is going to be made public any time soon or any time in the near future.

Senator KYL. Well, they would need a lot better assurance than that, though.

Mr. GONZALEZ. That is generally—that is our process.

The other thing that I would intimate is there is a particular case that I am pretty sure has been resolved where a bank, in fact, was defrauded of about 10 or so million dollars, and we were able to recover all that money based on the company's willingness to report. I think we recovered all but $800,000 of the $10 million or so that were taken.

So I think the upside or the benefits to private industry and to these companies that have the potential of being defrauded is much better in joining forces with law enforcement to try to resolve the issue as opposed to not reporting.

Senator KYL. I believe that, you believe that, and it makes intuitively good sense. Obviously, it is going to be necessary to continue to operate in a way that assures the public that this kind of protection of their sensitive information will occur with law enforcement so that they will have an incentive to fully cooperate.

Let me ask you about the arrest earlier this year. Maybe you are not totally familiar with the inside details of it, but perhaps you could share some information with us here about the Canadian law enforcement officials' arrest of the young man in Canada, a 15-year-old teenager, as I understand it, who is suspected of being at least one of the people responsible for the recent denial-of-service attacks on the Internet sites in the United States. Can you tell us a little bit more about how the investigation of that case was conducted by the FBI and what the status of it is?

Mr. GONZALEZ. I can tell you in general terms the processes that we went through that I think resulted in some of the successes.

First of all, there was an almost immediate reporting of the intrusions or the denial-of-service attacks by the companies affected, which obviously triggered a response from the FBI. With the FBI's structure as it is nationwide, where we have nationwide offices, in each of those offices we may not have fully fledged computer intrusion squads, but we have agents that are assigned to those matters across the country. We were able to almost simultaneously develop information that had leads, as we call them, all over the country and able to address those simultaneously with the use of the National Infrastructure Protection Center, which one of their roles is the coordination of these types of investigations because of their national scope and international scope.

So all those things occurred almost, again, I will use the term simultaneously, because once it was reported, it put several processes into action, including the coordination efforts by NIPC, the individual field divisions getting out and addressing the particular leads they had, which we had some in Phoenix, and at the same time, once it was determined that there was a nexus to Canada, our legal attache office in Canada was able to have liaison with the RCMP and able to make the information either available or pass it and a lot for the successful processing of the information to the Canadian authorities so they could make the arrest.

But as you can see, it is a multifaceted process that we went through. It would be extremely difficult to do that if we didn't have the national resources available and on hand to conduct the adequate investigation.

Senator KYL. It sounds like another good example for the need for a multiple or nationwide trap and trace authority as well.

Mike Vatis in Washington, DC, in our hearing there, the Director of the FBI's National Information Protection Center, the NIPC——

Mr. GONZALEZ. Infrastructure.

Senator KYL. Yes, I misstated that. He discussed two programs called InfraGard and Key Asset Initiative. Can you describe those two programs and how they are being carried out here?

Mr. GONZALEZ. Yes, Sir. The Key Asset Initiative involves each field division of the FBI within their jurisdiction in identifying key assets that are involved, whether it be providing infrastructure services, whether it be communications, transportation, academia, identifying these assets and making contact with them and obtaining—and setting up with them a system whereby we have 24-hour points of contact with those different assets so that in the event there is either an intrusion or an attempted intrusion, that we can be—we will have access to those different entities.

The InfraGard program involves an information-sharing initiative that is coming out—that is actually in place in a lot of areas. We are getting ready to implement it in Arizona. But what we do is, we offer anonymity to any company that wants to join us, and it will do things. It will give them the ability to provide the FBI and NIPC with information regarding either intrusions or potential—or attempted intrusions into their system through an encrypted e-mail capability, and also as being part of that program, it will allow them to receive warnings or threat warnings or intrusion warnings from NIPC as they are doing their national review of these particular incidents.

So the Key Asset Initiative identifies areas in industry and in business that have potential for being either attacked or have potential of affecting our infrastructure and our commerce, and then the InfraGard initiative includes those entities and other entities in private business, private enterprise, that have a need to be advised of either threats or potential threats through the encrypted e-mail system.

Senator KYL. So are you actually going out to industry and visiting with them about their potential participation?

Mr. GONZALEZ. Yes, Sir. We are currently in the process of doing that.

Senator KYL. Let me ask each of you a last question just to indicate to the audience here we have to conclude the hearing by 11 o'clock. We have two more witnesses. So even though I can—I love getting information from these folks, and I could sit here all day. But we will have to close it off and move on to our next witnesses here.

But let me ask both of you, Attorney General Napolitano, you mentioned desk subpoenas in your testimony, and Director Louis Freeh testified about administrative subpoenas necessary to effectively track cyber crime. Could you describe what those are and how that relates to our need for modifying law or procedures?

Mr. GONZALEZ. In terms of the FBI, they are referred to as administrative subpoenas. The FBI currently has that and some other Federal law enforcement agencies have that ability in drug investigations, in health care fraud investigations, and in crimes against children investigations. It basically allows the head of an office or

one of his designees to issue a subpoena for information when it regards one of those types of investigations.

What that does, it is actually two-fold: Again, it goes to the timeliness. We have an ability to do that almost at a moment's notice if needed in a particular investigation; and, No. 2, the information we gain from those subpoenas, there are no restraints in terms of us sharing it with other State and local law enforcement agencies or anyone else that would have a need to know in terms of getting that information as opposed to comparing it to a Federal grand jury.

Senator KYL. Is there a difference between an administrative subpoena and a desk subpoena?

Ms. NAPOLITANO. Well, we use the term desk subpoena as shorthand for a subpoena that a prosecutor signs as opposed to continually going back to the grand jury to get another subpoena *duces tecum*. So what Arizona law will provide when this provision takes effect is that on the certification of the prosecutor that this is relevant to an ongoing criminal investigation, we can issue based on that signature on a subpoena *duces tecum* to a service provider without having to continually go back to the grand jury and get a subpoena. It is very important because in a lot of these cases, as you see, we are following, say, for example, an e-mail to its source, and we can literally go around the country and end up in Glendale. But this way we can do it very quickly. We can do it at night. We can do it on weekends when the grand jury is not in session, and oftentimes we need to be able to do that.

Senator KYL. And the legal protection is that the evidence is obviously not usable if it has exceeded the probable cause requirements that you would ordinarily have to seek from a judge.

Ms. NAPOLITANO. Right. And the purpose is not to get the content of the e-mail. This is simply to be able to track where it—the chain of where it is coming from. So that is the primary purpose of this, not to get the actual content but to be able to find out the source of the e-mail. And as I mentioned earlier, Senator, many times we have to do that at night and over the weekends where continually going back to get a subpoena is impossible.

Senator KYL. I hope if our viewers have picked up anything from this hearing, they will appreciate the challenge that law enforcement is faced with in investigating these kinds of crimes because of the huge technological challenges that are presented and the very limited resources that you alluded to, Ms. Napolitano, and some of the legal—the very strict legal requirements that we impose in this country to make sure that people's constitutional rights are not in any way invaded, and that sets up some very high barriers for law enforcement but that obviously we intend to continue to abide by those requirements. It makes it tough for law enforcement, but you can still get your job done if you have adequate cooperation with the people who are reporting the crimes, and from the Congress perhaps and the State legislature, as you have noted, in providing the kind of legal authority and resources necessary to do the job.

It is a very difficult challenge. It will evolve as time goes on, and I commend both of you and your offices for the way that you have jumped on this very quickly. And certainly as you have pointed out,

General Napolitano, Arizona being the leader in developing both the legal authority and within your office the ability to quickly deal with these kinds of cyber attacks.

I commend you both, and I appreciate you testifying here. We will have the record open for a period of time for any other comments you would like to make, and naturally I am always appreciative of your advice on the subject. So thank you very, very much.

Mr. GONZALEZ. Thank you.

Ms. NAPOLITANO. Thank you, Senator.

Senator KYL. Our next witness is David Aucsmith, the chief security architect for the Intel Corporation. Mr. Aucsmith is a recognized expert in the computer security field and will be making the U.S. industry presentation at the upcoming G–8 summit on cyber crime in May in Paris, France.

Mr. Aucsmith, your full statement will be placed in the record, and I would invite you to make summary remarks at this time. And, again, I very much appreciate your presence here.

PANEL CONSISTING OF DAVID W. AUCSMITH, CHIEF SECURITY ARCHITECT, INTEL CORP.; AND JOSE GRANADO, SENIOR MANAGER, ERNST & YOUNG LLP, HOUSTON, TX

STATEMENT OF DAVID W. AUCSMITH

Mr. AUCSMITH. Thank you very much, Senator.

The purpose, I think, of my presentation is to talk about the technological trends and challenges facing the protection of critical infrastructures as we move forward.

Intel's former CEO, Andy Grove, was very fond of starting a lot of his presentations with the statement that we are rapidly approaching a time of a billion connected computers. That is actually a fairly fantastic statement. He said there are roughly a billion connected computers simultaneously exchanging data. And the computers that we are talking about are not just PC's. As was mentioned earlier, we are talking about the controls to an irrigation system. We are talking about national power grids, airline reservations, financial information from Wall Street, accessible by a billion connected computers.

Why is this done? The obvious reason is to improve cost and efficiency. It lowers the cost if there are common infrastructures allowing communications and information to take place, and it significantly raises the efficiency. In fact, a year or so ago, the Department of Commerce credited that efficiency with keeping the level of inflation a whole percentage point lower than it would have been otherwise.

However, this same efficiency also created quite a number of vulnerabilities, which is what this hearing is basically about. Those efficiencies mean that we have just-in-time inventory management, we have just-in-time commission and movement. That leaves very, very little room for error when that system is disrupted. That just-in-time inventory also applies to critical components of the national power grid and transportation sectors.

Basically what we have seen so far is vandals on the Internet, as another way of putting it. That is the majority of the cases. If you have a billion connected computers, one way to look at that is

you have a billion minus one potential attackers to your particular computer system.

Another way from my end that we look at this is that we basically have a billion connected computers each of which has a billion different security policies. We actually can't seem to agree on precisely what is the right way to defend or to state even how we should defend each of the individuals sites.

The statistics are rather frightening. It includes major companies such as Intel and others attacked somewhere around the neighborhood of 6,000 a day. You have cable modem users who would reflect around 250 attacks or so a week. And it is a fairly phenomenal amount.

Now, most of these attacks are the equivalent of vandalism. I like to point out it is somewhat like spray painting in cyberspace. It is about the same equivalent. The problem, of course, is that you really can't tell which of those are potential spray painters and which of those are potentially serious fraud or an intelligence-gathering operation.

One way to look at it is if you were a business you wouldn't tolerate a few thousand people a day walking up and rattling your front doors or trying to see if there is an open window where they could come into your business, yet in cyberspace, we have sort of grown up and accept these just as a matter of fact. We can't live with this as a basic problem. In fact, when vandalism gets out of hand, you end up with the distributed denial-of-service attacks that we have just had. That's what happens if several thousand people show up at your front door at once.

There are other problems which is just essentially the cascading destruction that occurs when one part of the system fails due to a vandalism or a malicious attack or a terrorist incident or whatever. The interconnectivity causes a great deal of things to happen all through.

But I don't want to dwell on vandalism. There is a great statement from the bank robber of the 1950's, Willie Sutton. When he was asked why did he rob banks, he said, "Because that's where the money is." Well, right now e-commerce is where the money is. In fact, it is very likely that we will see serious criminals—and we are beginning to see them—move into cyberspace because that is where the money is.

We have seen this in the case of credit card theft and a number of others. Basically cyberspace offers precisely the two things that criminals need: anonymity and mobility. Those happen to be the things that generally e-commerce also needs, but they do facilitate the bad guys.

Most security domains as they are set up now approach what we call the nougat method of security, which is they have a very hard shell on the outside and they are soft and chewy on the inside. So all you have to do is break through that outer barrier and people do not practice defense in depth in general.

That is not to say that people aren't trying. There is a great deal of standards development going on within the industry. The international standards is essentially the glue that binds cyberspace together, and there is a lot of work, including IP security standards for telecommunications, use of better identification methods like

smart cards and biometrics. All of those things are happening, but it is important to stress that standards development is extremely slow. Because it is an international endeavor, it does not move at cyber speed.

Also, security is traditionally a form of insurance. We didn't put up metal detectors in airports until after airlines were hijacked. We are unlikely to put in strong security in cyberspace until after major incidents. It is just very hard to get people motivated otherwise.

One of the perhaps best things that we can do is to provide some assistance for law enforcement and others in dealing with the current problems. The technology that we deal with is extremely complex. Its very efficiencies frequently frustrate the ability to catch criminals in cyberspace. It is complex and esoteric. Experts typically are hard to find and have to be paid a great deal. It is very difficult for law enforcement to deal with that.

Intel might be regarded as being at the forefront of this technological revolution, certainly one of the companies, and it is very difficult for us to keep up with the technology, and we dedicate a great number of people to doing that.

The best thing that we can do is to have good cooperation amongst industry components and with governments to help make the Internet a safer place and to protect the critical infrastructures. There are several good examples of that cooperative effort. Some of them have already been alluded to. There are others such as the information technology study group, which is a joint industry and FBI initiative to look at strategic directions in solving these problems.

However, there are problems with that cooperation. Some of them have been alluded to. We are now having a collection of industry competitors coming together to share information. That brings up antitrust issues. Certainly from the strategic standpoint, we have companies disclosing vulnerabilities and other intellectual property about their products that is subject to discovery and may end up in a court of law. That is not something generally wanted by industry.

There are problems with funding of those cooperative efforts. Industry is pretty much consenting to do this on a *pro bono* basis, *gratis*, if you will, but the government sectors of those require funding in order to do the Administration and make the best use of that.

Congress also will have to address other problems. The biggest problem looming on the horizon is that having to do with jurisdictional issues. Cyber crime occurs all over the world. It is very difficult to figure out who exactly has jurisdiction and in what cases. Some of that is being addressed.

So, basically, in closing, though I don't want to leave you with too bleak a view here, the technology is basically amoral. It is just moving at a very rapid pace. It is being used for good and, of course, bad guys will move in, too. Traditionally, law enforcement and national security interests have been able to adapt to changes in technology from the automobile, the telephone, and others over time. I am sure that in time we will be able to adapt to create effective order in the new technologies. It is perhaps fitting, if you

will, that this is being held in Arizona. It somewhat resembles the Wild West at this point of view, and it is merely a need to slowly but surely civilize it. That is one way to look at it.

Thank you very much, Senator.

[The prepared statement of Mr. Aucsmith follows:]

Testimony of David W. Aucsmith,
Chief Security Architect, Intel Corporation
Before Senator Jon Kyl, Chairman of the
Subcommittee on Technology, Terrorism, and Government Information of the
Senate Judiciary Committee
April 21, 2000

Thank you Senator Kyl for the opportunity to testify on the important topic of cyber security. My name is David Aucsmith, and I serve as Chief Security Architect for Intel Corporation. In this capacity, I am responsible for data and communications security in Intel products and services. I also serve as the technical liaison to the law enforcement and intelligence communities. My background prior to joining Intel includes over twenty years of service in both the government and private sector in the fields of information security and cryptography.

At the outset, let me say a few words about Intel. Intel is the world's largest semiconductor manufacturer and a leading producer of computer, networking and communications building blocks to the Internet economy. Intel's flagship business continues to be the mass production and sale of the Pentium® processor family and other microprocessors. At the same time, our business is expanding beyond supplying the PC industry with chips and related printed circuit boards to providing Internet solutions in such areas as wireless products, networks and communications, and on-line services. In 1999, our sales exceeded $29 billion.

Cyber security plays a major role in the conduct and growth of Intel's business. The ability to safeguard networks and information systems on a global basis is increasingly critical to internal company operations, intellectual property protection, e-business, and on-line services. This trend is graphically illustrated by Intel's e-commerce activities, which have skyrocketed from zero to $1 billion in monthly sales over the last few years. In addition, user requirements for on-line security have led Intel to pursue security as a commodity feature of information technology (IT) products, an endeavor greatly facilitated by the Administration's recent encryption policy reforms. For example, in May, we will make source code for strong Intel security software freely available on the Internet, increasing industry capability to build IT products with security management capabilities.

The importance of cyber security is especially relevant to critical infrastructures upon which companies like Intel must rely. As with the public, Intel relies heavily on stable telecommunications, transportation, energy, water, banking and other infrastructures. These infrastructures are largely and increasingly dependent on networks and information systems. It is therefore in Intel's vested interest to help prevent destabilizing cyber attacks on critical infrastructures to the greatest extent possible.

Today, my testimony will reflect Intel's strong dedication to cyber security by addressing three areas applicable to any consideration of security threats and countermeasures:

- IT industry trends in addressing cyber security challenges
- The role of industry and government in addressing threats to cyber security
- Recommended course of action

I. IT Industry Trends in Addressing Cyber Security Challenges

A. Need for a Secure Information Infrastructure

Today's global information infrastructure is characterized by more than 95 million network-connected computers, most of which are located in open environments with little or no physical control. This infrastructure cuts across all other critical infrastructures. Indeed, interconnected computers are used to control defense facilities, energy grids, financial institutions, the telephone system, industry and government networks, e-commerce and much more. The global information infrastructure has essentially become permanently interwoven into the fabric of our daily lives.

The following statistics, based on the American Electronic Association's recent report entitled Cybernation 2.0, illustrate the ever-increasing pervasiveness of the information infrastructure throughout the world:

Computers in Use by Regional Groupings (in thousands)

REGION	1993	2000	Percent Change 1993-2000
North America	83,391	182,600	119%
EU	44,283	134, 559	204%
European Free Trade Ass'n	1,888	6,157	226%
Central & Eastern Europe	2,169	11,913	449%
Asia-Pacific	24, 972	115, 581	363%
Latin America	3,121	17, 963	476%
Other	11,528	60,910	428%
World Total	171,352	529,683	209%

Source: Computer Industry Almanac, Inc.

Internet Users by Regional Groupings (in thousands)

REGION	1998	2000	Percent Change 1998-2000
North America	83,656	148,980	78%
EU	31,296	79,282	153%
European Free Trade Ass'n	2,434	4,774	96%
Central & Eastern Europe	1,667	4,699	180%
Asia-Pacific	21,466	50,512	135%
Latin America	1,742	7,194	313%
Other	7,143	20,407	186%
World Total	149,404	315,848	111%

Source: Computer Industry Almanac, Inc.

The rise of the global information infrastructure is having enormously positive transformational effects on society. It is creating scale economies and expanded information-based capabilities that are improving commerce, business, education, health care, defense, the media and many

other sectors. The impact of this transformation has been so profound that many now talk in terms of the "Internet" or "new" economy versus the "old" economy.

The viability of the networked world is dependent on user trust and confidence in networks and associated information systems. Along with privacy, cyber security is a key enabler of user trust and confidence. It is required to safeguard the storage and transmission of data against malicious hackers and others that engage in activities ranging from credit card fraud to stealing trade secrets to disrupting the operation of critical infrastructures.

It is thus in industry's self-interest to promote cyber security measures to the maximum extent possible, taking into account the need for corporate and personal privacy. What are the industry trends and challenges in this vital area? The question requires answers in several contexts, including security technologies/products, security standards, best practices, and information-sharing on cyber threats.

Security Technologies/Products. Presently, global networks use a wide variety of software and hardware with no common security policy. While some hardware and software security products have been available on a mass-market basis, security products have not generally been cost effective, typically filling only niche markets. Furthermore, the lack of integration and interoperability of security tools with other network management tools means that security products cannot be successfully incorporated into modern remote support strategies. Most companies leave security management and monitoring plans on the shelf for just this reason.

Meanwhile, both the value and volume of on-line information has sharply risen. This includes organizational information such as financial data, manufacturing information, customer information, medical and legal records, and human resources data. Additionally, there is a growing amount of data which has intrinsic value, such as monetary instruments (e.g., credit cards, coupons, etc.) and intellectual property (e.g., movies, images, etc.).

The availability of on-line security services and security products like intrusion detection, anti-virus and encryption software is nevertheless growing. Ultimately, the inexorable need for secure networks and systems is likely to make security a commodity feature of IT products and information services. But integration and interoperability challenges must be overcome to successfully enable security implementations at the organizational level.

Security Standards. Today, communications security is being addressed by IP/SEC (Internet Protocol Security), SSL (Secure Sockets Layer) and authentication methodologies that employ smart cards and biometrics. IP/SEC, which protects Internet data, has been under development over the last 5 years within a body known as the Internet Engineering Task Force. Some 50 vendors now supply IP/SEC-compliant products. Meanwhile, SSL has become a widely accepted standard for e-commerce and is typically represented by a lock on browsers. As for authentication methodologies, international consortia are now working on the interoperability of smart cards to ensure high resistance to attacks. The effort includes work on standardizing biometrics, such as fingerprint and face recognition.

While the above standards are applicable to e-commerce, they are finding their way into other applications as well. For example, the military is using smart cards for ID purposes.

The key to quick and broad implementation of security solutions is fast turn-around in the standards-setting process. Uniform standards are needed to promote integration and interoperability of security products with existing infrastructures. Today, standard-setting is an

international process driven by divergent market and political forces. The process is therefore ad hoc, slow and unpredictable by nature.

Best Practices. Recent cyber attacks have precipitated considerable discussion over the need for workable security practices by government and the private sector. Increasingly, there is recognition that users must deploy authentication, encryption, firewalls or other technologies as well as smarter on-line behaviors to thwart cyber attacks. To the extent users are educated on best security practices, they will be able to deploy countermeasures that reduce threats and vulnerabilities.

However, network attacks cannot be totally prevented. Hackers will always find software or system flaws to exploit. Thus, security products and best practices may well have to be supplemented by security services that provide continually updated and real-time detection and response capability. The problem is akin to an arms race in which one side must always update technological capabilities and behavioral patterns to keep ahead of the other side.

Information Sharing. The White House publication "National Plan for Information Systems" makes it clear that all cyber security stakeholders must coordinate together to counter threats and vulnerabilities. Such coordination is already underway. In recent months, the broad-based Partnership for Critical Infrastructure Security was established to help provide solutions to infrastructure security problems. The partnership consists of representatives of many companies, trade associations and federal departments and agencies.

Sharing of knowledge among partnership stakeholders is a key priority for dealing with information attacks and vulnerabilities. Under the auspices of the Information Technology Association of America, many companies from the information and communications sectors are already working to establish a mechanism for the systematic and protected coordination of information regarding cyber attacks, vulnerabilities, countermeasures and best practices. This should provide an effective early warning system over time, provide that antitrust or other barriers to information sharing can be overcome.

B. Technological Trends and Law Enforcement

The very technologies that empower computers, networks and security capabilities have a direct impact on law enforcement's ability to access plaintext communications or stored data. These technologies are a function of strong forces for technological innovation. The same innovation that has brought the richness and efficiency of the connected world has also brought challenges to the "old" ways of conducting business – including the business of law enforcement.

Digitalization

Clearly the most dramatic trend is the movement from analogue to digital representations of information. Any information can and will be represented in digital form. Digital information can be stored and transmitted with no loss of content or fidelity. It can be easily manipulated and replicated. The ease in manipulation means that information can be easily transformed into representations that are difficult to detect or understand unless complete knowledge of the transformation is available. Digital voice, for example, is indistinguishable from digital stock quotes if the transformation and protocol are unknown. In the end, "bits are just bits."

Cryptography

Only cryptographic technologies are capable of projecting security onto the completely open, arbitrary environment that is the Internet. Cryptography, by itself, does not guarantee any level of

security. It is a necessary component but not a sufficient component. It can provide the essential component of authentication, confidentiality, and integrity. It can guard intellectual property and ensure that a banking transaction is not fraudulent. It can also shield child pornography and keep a drug deal secret. Overall, there are significant forces propelling the wide use of cryptographic technology such as the IP/SEC standard and the Advanced Encryption Standard from NIST.

Digital Modem Protocols

Computational bandwidth is increasing at a substantially greater rate than communications bandwidth. This inequality favors trading off more strenuous computation for more effective communications bandwidth utilization. There are several technologies currently under development to maximize communications channel utilization that will pose serious barriers to communications intercept.

Data Specific Compression Algorithms

Many data-specific communications protocols, such as the H.323 video conferencing protocol, contain data specific compression algorithms (e.g., MPEG) which, without knowledge of the type of data being exchanged, resemble encryption at the point of intercept. Again, in order to maximize communications bandwidth, the trend is toward the development of data-specific compression that effectively renders data communications intercept unreadable.

Multiple Communications Paths

One way of overcoming communications channel bandwidth constraints is to utilize multiple communications channels. There are many commercial developments underway to use non-traditional communications channels for data communications, such as cable TV, satellite broadcast, and the electrical distribution system. Interception of communications at the "common carrier" may require access to many different communications infrastructures. Interception will be made even more difficult when the individual packets of a given communications session are dispersed among a wide range of infrastructures.

Steganography

There has been active academic research into stenographic communications protocols. These protocols pose perhaps a greater barrier to interception of plaintext communications than does cryptography. By their design, they prevent an eavesdropper from being able to detect the very existence of information being communicated between two or more parties.

Voice Over IP

Perhaps the most significant technological trend confronting law enforcement is the move towards voice communications over the Internet. This will render most of the established voice interception methods ineffective and will allow all of the other technical trends to apply to normal voice communication such as encryption, compression, multiple communications paths and steganography.

New challenges. The challenge for law enforcement is to adapt to changing technology and find, within it, the means to perform their job. This is not the first time that this has happened. Throughout history, law enforcement has needed to adapt to new technology. It adapted to both the automobile and the telephone over time. The difference today, with the Internet and computers, is merely in the degree of complexity of the technology and the speed of implementation.

Once the technology and its evolution are understood, there are opportunities for both lawful interception and seizure of evidence. The problem faced by law enforcement is not one of unsympathetic technology but, rather, a lack of expertise and resources.

Technogical Solutions. Dealing with technological change is a daunting task – even for those immersed in its day-to-day creation. This is especially true for law enforcement because:

- The technology changes more rapidly than any published information about it
- The general direction of technology can only be comprehended with a visibility into many diverse industry standards activities
- The complexity of much of the technology is only comprehendible to experts.
- Technology experts are in great demand and frequently command financial compensation well above that which could be offered by law enforcement organizations
- Mandating technology solutions to solve law enforcement problems relative to information technology does not work (for reasons explained later in this testimony).

Clearly the only solution that makes sense is for those who create technology to team up with those who must use that technology to enforce the law. There must be a continued information flow from industry to the government if there is to be a viable option for achieving lawful access to plaintext data. Such an arrangement already exists informally by way of a joint industry / FBI cooperative effort known as the Information Technology Study Group. All that is left is for congress to adequately fund a technical support center that formalizes this arrangement.

II. Role of Industry and Government in Addressing Cyber Security Threats

A. Cyber Security Efforts Should Be Industry-Led

As recent Internet viruses and denial of service attacks have reminded us, more needs to be done to secure the information systems that many sectors of the U.S. economy (utilities, banking, communications, transportation, health care, e-commerce) as well as the U.S. government rely upon extensively. Protecting the information infrastructure used for these critical sectors is essential to U.S. national security, American economic welfare, and our fundamental freedoms.

Intel believes that critical information infrastructure protection (CIIP) is best accomplished through private sector solutions that are market driven and industry led. The private sector not only builds and maintains the products, networks, and systems that make up the information infrastructure but also possesses the knowledge and expertise necessary to protect it.

As noted earlier, it is in industry's self-interest to protect the networks and information systems that form the backbone of critical infrastructures. For instance, safeguarding the privacy and security of every member of the Internet community is top priority at Intel. Such protection is essential to the future growth of the Internet and e-business. Without it, user trust and confidence in "the networked world" will wane, jeopardizing the economic health of IT companies.

B. Government Should Play a Supportive Role

Intel believes the U.S. government should support industry efforts to secure information-based infrastructures. Government support should include facilitating industry sharing of knowledge on cyber threats, vulnerabilities and countermeasures. It should entail measures to protect the

privacy and security of government computer systems and networks using industry best practices. It should include sharing results of government-funded cyber security research with industry and encourage academic research. Finally, it should involve punishment of cyber crimes by aggressively enforcing criminal and civil laws.

Importantly, the U.S. government has so far recognized that it should work cooperatively with industry on a voluntary basis to deter, identify and respond to cyber threats and attacks. The Administration has also proposed -- and Congress has funded -- numerous initiatives to strengthen the government's technological capabilities.

C. Government Policies Must be Workable

Intel applauds the Administration's current cyber security initiatives and will cooperate with the government in their implementation. However, Intel is concerned about possible overreaction to denial-of-service or other potential cyber attacks. Such overreaction could generate new laws or regulations that would stifle innovation, artificially channel R&D, and harm the very infrastructure that needs protection.

It is essential that the government not use legitimate threats to cyber security as a justification for assuming broad new powers of regulation, imposing new burdens upon industry, or threatening fundamental rights of privacy. As a matter of practice, the government should only pass new laws or adopt new regulations where it is demonstrated that current legal regimes are inadequate. Any new legal requirements, however, should not mandate information tracking, access requirements or other capabilities/standards for IT technologies. The government must also not engage in broad surveillance of networks and information systems. There are several reasons for these caveats:

- Technology mandates are technologically unworkable in the IT industry. The IT industry is characterized by an open, international horizontal architecture that makes one-size-fits all solutions (like built-in access capability) technologically unworkable. Unlike the centralized telecom infrastructure, there is no "top-down" control of information technology products and related networks. Further, uniform adoption of special product protocols in IT environment is extremely difficult because standards-setting is largely ad hoc, decentralized and global. Thus, by definition, technology mandates cannot succeed because there is no binding mechanism to ensure that all IT architectural layers (from components to computer platforms to operating systems to network protocols) will comply with government requirements.

  (NOTE: Rapid technological advances compound the problem. Assuming the government chose to mandate technological requirements, advances in technology would soon outpace the scope of those requirements, creating the need for new regulations on a continuous basis. This would spawn an unworkable regulatory treadmill.)

- Global IT standards are highly unlikely to embrace mandated tracking or access capabilities in any case. Government-mandated tracking or access capabilities create information vulnerabilities that threaten IT security and consumer privacy. Global marketplace acceptance of products and commercial infrastructure featuring such capabilities is therefore very unlikely. Absent market acceptance, there will be no impetus for adoption of enabling technology standards. One standards body, the Internet Engineering Task Force, has already rejected imposition of CALEA (Communications Assistance for Law Enforcement Access) standards for the Internet.

- Broad on-line surveillance will undermine trust and confidence in the Internet, the economic backbone of the IT industry. If users perceive that security and privacy on the Internet are being compromised by broad government surveillance activities, they will likely choose to avoid this medium. This could have profoundly negative economic consequences for the IT industry and the Internet economy as a whole, since innovation and development of IT products is now largely driven by Internet growth.

III. Recommended Course of Action

Intel believes efforts to address cyber security threats, vulnerabilities and countermeasures should rest on a firm set of principles. In particular, we endorse the principles adopted by Americans for Computer Privacy (ACP) to guide government decision-makers. ACP is a broad-based coalition that brings together more than 100 companies and 40 associations representing financial services, manufacturing, telecommunications, high-tech and transportation, as well as law enforcement, civil-liberty, pro-family and taxpayer groups. The ACP principles are as follows:

1. CIIP is best accomplished through private sector solutions that are market driven and industry led;
2. Governments and industry must work cooperatively on a voluntary basis towards achieving CIIP;
3. Government must not mandate the choice of technologies or dictate standards or processes;
4. Government must not violate personal and corporate privacy in the quest for CIIP; and
5. Barriers to strong CIIP should be removed, including barriers to the widespread use of strong encryption.

Based on these principles, Intel believes that the model for undertaking CIIP efforts should include the following elements:

RESPONSIBILITY	ACTION
IT Industry	Develop best cyber security practices
IT Industry/Academia/Government	Educate public on risks and safeguards
IT Industry	Develop and deliver security technologies/tools
IT Industry/Academia	Perform R&D to address threats and develop solutions
IT Industry	Establish knowledge-sharing mechanism within industry to address threats, vulnerabilities and countermeasures. Enlist support from government and academia.
Government	Remove antitrust or other barriers to industry knowledge-sharing
Government/Industry	Provide scholarships to increase America's security workforce and related expertise
Government	Provide appropriations to safeguard government networks – i.e., make sure the government's "house" is in order.

RESPONSIBILITY	ACTION
Government	Provide appropriations for government-sponsored R&D that can be shared with private industry.
Industry	Share expertise with government to address crime in a digital world.
Government	Fund a technical support center to carry out the above sharing of expertise on a systematic basis.
Individuals, Consumers, Businesses	Increase security expertise; use best practices, tools and services provided by the IT industry.

This model, while illustrative rather than comprehensive, is an attempt to recognize the recurrent and evolving nature of cyber threats. Accordingly, it establishes remedies that systematically address problems over time.

We urge you to consider the merits of this approach as you continue your efforts to address the cyber security issues.

Thank you, Senator Kyl, for the opportunity to testify at this important hearing today. I will be glad to respond to any questions that you may have.

Senator KYL. Well, thank you very much, Mr. Aucsmith. Of course, we wanted to put one of our premier corporations on display as well, and since you are a leading technology expert in the area, we thought this would be a good forum in which to discuss this. I am not sure whether we should have had you before or after our next witness, though, because our next witness is going to demonstrate to us how this hacking is done.

Now, I have some assurances that with the law enforcement officials here, this will all be done in a quasi-legal way, but I take no—I give no assurances in that regard. Let me properly introduce to you Jose Granado. He is a senior manager at Ernst & Young, a highly qualified accounting firm in the country, no fly-by-night hacking outfit, I would hasten to point out. And recently it was named as the outstanding information security organization, as I understand it, by the Information Systems Security Association. So Jose also comes by his expertise rightly.

He has been involved with information security for the last 12 years. He is a frequent speaker on the topic. We thank you for testifying today, and as I have mentioned to the others, your full statement will be placed in the record, and we would appreciate a summary of your remarks at this time.

STATEMENT OF JOSE GRANADO

Mr. GRANADO. Good morning, Mr. Chairman. Thank you for the opportunity to testify today regarding improving prevention and prosecution against cyber attacks. As you mentioned, I am a senior manager with Ernst & Young's eSecurity Services group. I direct a team of "white hat hackers" who perform network assessments on client networks. Their objective is to identify existing weaknesses in computer systems that will lead to unauthorized access. My perspective comes from having led over 100 network security assessments over the past several years. Assisting me today is Ron Nguyen, a manager with our eSecurity Services group. Today we will describe and demonstrate the process we utilize to perform these assessments.

When performing these assessments, we obtain a snapshot in time of an organization's network security posture. This snapshot allows us to identify potential points of entry to gain unauthorized access to a network. The demand for these assessments has been generated by several factors: increased e-commerce initiatives, increased Internet dependency, which has generated a need for independent security reviews, increased discovery of operating system and application level vulnerabilities, and increased publicity, as we have seen recently with the denial-of-service attacks on eBay, Yahoo, and others.

Although our team is extremely skilled, over 75 percent of our initial access into client networks is gained via relatively simple methods and techniques. Our success is facilitated by three factors: poor selection of user ID's and passwords, poor system configuration from a security perspective, and the inability for organizations to implement solutions on a realtime basis to existing vulnerabilities.

Hundreds of websites exist that contain system security information. The network used to exchange this type of information tran-

scends physical, geographical, and cultural boundaries. Internet chat sites, informal gatherings, and conferences also help to facilitate the flow of information.

During today's online demonstration, we will identify a live computer system, scan the computer system for potential entry points, gain access to the system, eavesdrop and control the system remotely, crack the password file, and, finally, execute a denial-of-service attack.

Our demonstration network is comprised of two Windows NT laptop computers. The computer labeled "attack," the one on the larger screen, will be performing the hacking activity. The computer labeled "victim," the one on the smaller screen, will be the recipient of the attacks. Although these computers comprise their own mini network, the techniques demonstrated today can be performed against any live computer on the Internet that is in a similar security state as our victim system.

An attacker can run a ping utility to randomly identify a range of targets on the Internet. The attacker can also target a specific victim to attack. For our demonstration, we will ping www.victim.com.

The ping utility has identified one live system on our network designated by the IP address 192.168.10.10. An IP address is a numerical designation that identifies a computer on a network. Once we identify a live target, there are a number of freely available vulnerability scanning tools that can be used to identify potential entry points. For our demonstration, we will use the freeware tool called "Superscan" on our attack system to scan our victim.

The scanner has identified potential entry points on our target system—specifically, ports 21, 80, 135, and 139. A port is a numerical designation for a specific network function. Part of the system access process is mapping vulnerabilities associated with these open ports to exploit tools. Our scan identified port 80, which is associated with Web browsing, as open. For our demonstration, we will launch the iishack tool on our attack system to gain access to our victim.

We now have gained access to our victim system. The attack was successful. The iishack tool the attacker used exploited a buffer overflow vulnerability on the target system. A buffer overflow condition is caused by the transmission of unexpected data to a target system, causing it to accept commands from an attack system. The hack tool launched a listening service that the attacker can now use to remotely control the system. This listening service allows the attacker to eavesdrop on the victim system by using a standard Web browser. For our demonstration, the attack system will monitor a letter being typed by the victim system.

As you can see, the attack system now actually has the screen of the victim system displayed on it. The victim computer is typing a letter with the notepad function, and what he is typing keystroke by keystroke is now appearing on the bigger screen, which is the attack system.

With remote control access, the attacker can leverage the target system as a launchpad to attack other systems, start programs, access and view files. For our demonstration, we will access and view files on the victim system from our attack system.

As you can see, the attack system here is going through the contents of the C drive on the victim system and actually bringing up documents that are on the victim system and actually appearing on the screen of the attack system. The documents, as you can see, appear in their complete entirety.

Now that the attacker has full control of the target system, one of the most popular activities is password cracking. The attacker can download the password file from the remote system and run a password cracker to discover user passwords. For our demonstration, we will download the password file to our attack system and using the lopht crack program demonstrate how quickly passwords can be cracked.

We have located the password file on the victim system. We have dragged it to the desktop of our attack system. We are now bringing up the lopht crack tool and feeding that password file to the cracking tool. And as you can see, in a matter of seconds 18 of 21 passwords were cracked, and that took probably 2 or 3 seconds.

If the attacker is simply looking for targets to crash, they can easily launch a denial-of-service attack directed specifically at the target system. For our demonstration today, we will launch a denial-of-service attack on our attack system to disable our victim.

The IP address of the victim system is being inputted into the denial-of-service tool, and after pressing the nuke button, we see that our victim system has been disabled as evidenced by the blue screen with all the error messages that are on it. And now that that system is disabled, it needs to be restarted to get back to its original state.

Thank you for the opportunity to testify today at this hearing, and subject to your questions, this concludes our quick demonstration.

[The prepared statement of Mr. Granado follows:]

PREPARED STATEMENT OF JOSE GRANADO

POWERPOINT TITLE SLIDE

Introduction

Mr. Chairman and distinguished members of the Subcommittee, thank you for the opportunity to testify today regarding improving prevention and prosecution against Cyber Attacks.

My name is Jose Granado. I am a Senior Manager with Ernst & Young's eSecurity Services group. I direct a team of "white hat hackers" who perform network assessments on client networks. Their objective is to identify existing weaknesses in computer systems that will lead to unauthorized access. My perspective comes from having led over 100 network security assessments over the past several years. Assisting me today is Ron Nguyen, a manager with our eSecurity Services group. Today we will describe and demonstrate the process we utilize to perform these assessments.

POWERPOINT SLIDE ONE

Introduction to White Hat Hacking

When performing these assessments we obtain a "snapshot" in time of an organization's network security posture. This snapshot allows us to identify potential points of entry to gain unauthorized access to a network. The demand for these assessments has been generated by several factors:

- Increased eCommerce initiatives.
- Increased Internet dependency—which has generated a need for independent security reviews.
- Increased discovery of operating system and application level vulnerabilities.

• Increased publicity—as we have seen recently with the Denial of Service Attacks on eBay, Yahoo and others.

Although our team is extremely skilled, over 75 percent of our initial access into client networks is gained via relatively simple methods and techniques. Our success is facilitated by three factors:

• Poor selection of userids and passwords.
• Poor system configuration from a security perspective.
• Challenges organizations face in keeping up the large volume of vulnerabilities discovered on a daily basis.

POWERPOINT SLIDE TWO

Hundreds of web sites exist that contain system security information. The network used to exchange this type of information transcends physical, geographical, and cultural boundaries. Internet Chat sites, informal gatherings and conferences also help to facilitate the flow of information.

POWERPOINT SLIDE THREE

During today's online demonstration we will:

• Identify a "live" computer system.
• Scan the computer system for potential entry points.
• Gain access to the system.
• Eavesdrop and control the system remotely.
• Crack the password file.
• Execute a denial of service attack.

START DEMO

Demonstration

Our demonstration network is comprised of 2 Windows NT laptop computers. The computer labeled "attack" will be performing the hacking activity. The computer labeled "victim" will be the recipient of the attacks. Although these computers comprise their own mini network, the techniques demonstrated today can be performed against any "live" computer on the Internet that is in a similar security state as our victim system.

Identifying a "live system"

An attacker can run a ping utility to randomly identify a range of targets on the Internet. The attacker can also target a specific victim to attack. For our demonstration we will ping *www.victim.com*.

Scanning a system for potential vulnerabilities

The ping utility has identified one live system on our network designated by the IP address 192.168.10. 10 An IP address is the numerical designation that identifies a computer on a network. Once we identify a live target, there are a number of freely available vulnerability scanning tools that can be used to identify potential entry points. For our demonstration, we will use the freeware tool "Superscan" on our attack system to scan our victim.

Gaining access to a system

The scanner has identified potential entry points on our target system. Specifically, ports 21, 80, 135 and 139. A port is a numerical designation for a specific network function. Part of the system access process is mapping vulnerabilities associated with these open ports to exploit tools. Our scan identified port 80 which is associated with web browsing as open. For our demonstration we will launch the iishack tool on our attack system to gain access to our victim.

Eavesdropping on a system remotely

The iishack tool the attacker used exploited a buffer overflow vulnerability on the target system. A buffer overflow condition is caused by the transmission of unexpected data to a target system, causing it to accept commands from an attack system. The hack tool launched a listening service that the attacker can now use to remotely control the system. This listening service allows the attacker to eavesdrop on the victim system by using a standard web browser. For our demonstration the attack system will monitor a letter typed by the victim system.

Controlling a system remotely

With remote control access, the attacker can leverage the target system as a launchpad to attack other systems, start programs, access and view files. For our

demonstration we will access and view files on the victim system from our attack system.

Cracking passwords

Now that the attacker has full control of the target system, one of the most popular activities is password cracking. The attacker can download the password file from the remote system, and run a password cracker to discover user passwords. For our demonstration we will download the password file to our attack system and using the lopht crack program demonstrate how quickly the passwords are cracked.

Executing a Denial of Service Attack

If the attacker is simply looking for targets to crash, they can easily launch a denial of service attack directed specifically at the target system. For our demonstration, we will launch a denial of service attack on our attack system to disable our victim.

Subject to any questions this concludes the presentation.

Senator KYL. Thank you very much.

Did the FBI get all of that down? [Laughter.]

You were taking good notes.

Obviously, this simulation attack is designed to illustrate how people with a little bit of expertise—and I know that our witness here has a lot of expertise, but I am going to ask him as kind of a first question how much expertise you need to do this—can quickly get into, can disable, can secure information from or deface a system, whether it be a business or commercial system, a government computer, a research or university computer, or certainly a private computer.

Let me begin by asking, Mr. Granado, just how experienced do you have to be to be able to do the kind of thing that you just now did?

Mr. GRANADO. The experience is not what one would think. We often find that individuals involved in this kind of activity have a love for technology. These are folks that stay up until 2, 3 or 4 a.m. reading everything they can get their hands on on systems and vulnerabilities and things of that nature. These kind of folks aren't individuals that have to go to Harvard to get this kind of experience. So the love for technology, a basic understanding of computer systems and networks is really at the foundation level all that is required.

Now, as I mentioned during my testimony, the voluminous amount of information that is out there on the Internet on how to go at these systems actually helps to facilitate the knowledge process for folks that want to get involved in this kind of activity. But the experience needed to do this is not great. It is just a general understanding of computers and networks, and then all the information that is available out there kind of helps snowball your experience level so that you can perform these kind of activities.

Senator KYL. I think illustrative of that is the fact that the first person arrested in connection with the denial of service of the various sites in the United States, the young Canadian, was 15 years old. And I will mention another operation. During the time the United States was preparing an attack on Iraq, there was an intrusion into some U.S. Government computers that was serious enough that it got the highest levels of our Government. We dubbed the exercise "Solar Sunrise." We eventually found that there were three people under the age of 20 in I think two different

countries that were involved in that attack. They were fortunately brought to justice.

But the point is that this seems to be coming a lot from young people who obviously don't have the college degree you are speaking of but have acquired the capability to cause great mischief.

Mr. GRANADO. Absolutely.

Senator KYL. Let me ask Mr. Aucsmith, at our hearing in Washington, DC, Harris Miller, who I am sure you know—he is president of the Information Technology Association of America—testified and he said one of the inhibitions of sharing information between the private sector and the Government regarding these vulnerabilities and threats is that companies naturally don't want their vulnerabilities and the attacks that have actually occurred against them to be publicly known since this could easily impact on consumer confidence in their particular sites and people then might not want to use their website. He said that unless companies are given an exemption from the Freedom of Information Act so that information they disclose to the Government can't be obtained by any other person that files the paperwork, that they would not want to voluntarily submit information to the Government in the name of cyber security.

Do you share this view? Do you think we need that kind of protection of private information from being acquired under the Freedom of Information Act?

Mr. AUCSMITH. Yes, Sir, I actually do, very much so. There are two issues at stake here, and it depends on for what the information is being used. If it is tactical information, the FBI may be needed to solve the problem.

Senator KYL. Meaning on how to—sort of to understand the kind of thing that Mr. Granado just now did, how does this system work so that we can track back the perpetrator.

Mr. AUCSMITH. Right. And for that, our concern is if we share that information, we may end up as a witness in a discovery process. No company wants to end up in a criminal proceeding with their product. The second, somewhat longer range, has to do with we are aware—as much as we may try, we can't produce perfectly secure systems. It is just not economically feasible. In many cases, it is not even technically feasible. So we are made aware of vulnerabilities, but we are sort of constantly trying to fix those vulnerabilities in each new product revolution. So what you basically have is a sliding window of vulnerabilities that go along, and industry is very reluctant to make that public because, clearly, that is only helping the bad guy. It certainly could be used by your competition to weaken your product. So there is some need—there is a need to come up with some solution for allowing—sharing the strategic vulnerabilities, helping your practical situation with knowledge that we have in a way that doesn't adversely affect the security of a company or the infrastructure that are built off of those products. Something needs to be done.

Senator KYL. Well, Congress is looking—I was involved in the Y2K legislation which gave some temporary time-outs for liability on sharing of information in order to ensure that in that run-up to the Y2K turnover that we wouldn't have an excess of problems. And that seemed to work pretty well.

So you would be supportive of Congress looking into the Freedom of Information Act, the potential for class action liability, antitrust liability, in a way to try to balance the need to share this information with the protections needed if the information is shared.

Mr. AUCSMITH. That is correct. Clearly, we are not advocating removal of FOIA. But what we are advocating is giving some level of protection where such vulnerabilities are so terribly sensitive.

Senator KYL. Now, Mr. Granado, one of the issues here is insider threat. In addition to hacking in from the outside, clearly there are some problems of the insiders. Could you comment a little bit about your concern there?

Mr. GRANADO. Yes, Sir, absolutely. I mentioned during my testimony that our access into computer networks 75 percent of the time is through simple methods and techniques, and that specific statistic was for attacks from the outside in. When we are invited into an organization to perform our assessments, our success rate is 100 percent. The reasoning there is obviously there is a certain level of trust that is assumed when an individual or a group of individuals are inside an organization, the security problem I think becomes twice as difficult because of that assumed level of trust, and the security controls that an organization implements, they need to be perimeter-based for external threat, but there also needs to be auditing and monitoring tools on the inside so that the activities of users on the inside could be monitored so that if any weird activities are occurring they can be flagged and acted upon.

Senator KYL. This is the so-called defense in depth concept that Mr. Aucsmith mentioned.

Mr. GRANADO. So there is no question that the insider threat is greater from my perspective than the outside threat. Again, that assumed level of trust of someone that you let inside your facility, they have already beaten one hurdle. They now just have to get to your network and access systems.

Senator KYL. I want to ask both of you a question here, and this goes right to the point Mr. Aucsmith made a minute ago. Maybe neither one of you want to reveal this nasty little secret to the public here, but I think it is important to do so in order to help do the job that both of you do.

I would like for you to describe just how vulnerable anyone on the Internet is, and let me put it in this context. Suppose I buy one of the new encryption products and let's call it pretty good security, and I buy that and I think, great, I am encrypted now, and unless some organization like the CIA tried to crack it, it is not going to be crackable. So I am home free here.

How foolish is that attitude? Just how vulnerable is anyone on the Internet? How easy is it and how many different ways are there to break into these kind of systems?

Mr. AUCSMITH. You have actually gone a reasonable step towards achieving security from a particular type of threat. That particular type of threat is collecting tactics at some intermediate point. What you have done nothing for is to protect the endpoint systems where that information originates or the destination of where it goes. In fact, given most encryption systems, the vulnerability is actually to break into the system and record the information before it is ever encrypted, which basically could be done in the attack you just saw

here, or to go hunting around in the computer itself for the keystrokes that were used to invoke the unknown—or the key, the encryption key. You would solve one of the problems, but probably not the hardest one, quite frankly. And how vulnerable are they? If you were to take this scenario that I just went through here, and instead of launching the particular attack I did, but start downloading the swap file, which is where the operating system puts intermediate material as it is being processed for efficiency, and then scan that for the invocation of your particular encryption program and the keystrokes that were used to invoke it, you will most likely recover the key.

Senator KYL. Can you describe this in terms of an analogy? I know you used the analogy of leaving the window open in the home. But can you think of a good analogy to bring home to people how you may have provided security at points D through F, but that is not all the way from A to Z.

Mr. AUCSMITH. The analogy that we frequently talk about is putting an armory on a screen door. I think basically you have armored the front door and left all the windows open.

Senator KYL. Mr. Granado, do you want to add anything to that?

Mr. GRANADO. Sure. The way I would like to comment on that, Senator, Ernst & Young is very active in providing this kind of information to the IT community. We have a website, www.esecurityonline.com, which provides vulnerability information for IT folks who are interested on what the latest threats are. And we also provide a separate section for clients. We give them customized vulnerability information based on the types of computers they have.

Anyway, my point is, for anyone to think that if they have a security product that they just purchased today and that makes them secure for the rest of time, it is extremely foolish. From a statistical perspective, we discover about 7 to 10 vulnerabilities a day that we either discover through our research labs or that we just gain information from other folks.

So as you can see, you think you are secure today, tomorrow, and the next day, but next week you may not be. You know, this issue is something that organizations need to consider a more proactive approach versus a reactive approach to security. And security is a process. It is not a matter of plugging a hole and then you are done. It is a process where you need to test, you need to implement solutions, and then you need to monitor those solutions. And that needs to be recurring. And that is the only way that we are going to be able to get ahead of the game with respect to these kinds of attacks.

Mr. AUCSMITH. Senator, one more follow-up to that. What the people from Ernst & Young are talking about is exactly correct. But I think we need to emphasize that the scenario they just painted is that for an IT organization or business. The same scenario is very difficult to work when you are talking about a home user. And one of our problems is my industry has been pushing very much to get everybody online all the time, always connected. We have been a little bit behind on sharing with them the vulnerabilities of being online and always connected. And the same set of methodologies that work for businesses are unlikely to work in the home

users. I can't imagine my mother being able to discern the information required to make a system secure.

So what we have to do as an industry is make security somewhat more seamless and automatic and easier to deal with. We have a ways to go on that. We are working very hard, but it is a very hard problem.

Senator KYL. I think that is a very candid and excellent statement of the state of play right now in the industry coming from one of the leading industry drivers here, acknowledging that in making this wonderful new tool so available to so many people so fast, we have got to catch up in terms of security and that that is going to require a significant degree of effort.

I think that our hearing today, if it will do nothing else, will be to demonstrate to people that there is a significant lack of security, but that shouldn't deter people from using the Internet, but that they should be very, very careful to the extent that what they have on there is private and they want to keep it private, and that industry generally and individuals are going to have to make good recommendations to the Government about what kind of protections they need in order to provide the fullest possible cooperation with law enforcement for law enforcement to do its job.

This is something that we want to do our best to cooperate on, and I just would reiterate to the audience here, my subcommittee deals with three subjects, and in this one area they all tie together: technology, terrorism, and Government information. And so we are right on the cusp of this. I have introduced several pieces of legislation, some of which have already been signed into law, some of which are pending, as you heard before, and designed to try to begin to resolve these issues. But perhaps the biggest point that I would make—and I would like to have the witnesses comment on this, and then we will—again, I could talk to these guys all day long. I wouldn't understand a lot of what they say, but I can at least appreciate the point they are trying to make. But we will need to cut our hearing off here in a moment.

We need to create an atmosphere of understanding and mutual commitment and trust that will enable private users, the private commercial sector, and the Government policymakers and Government law enforcement people to work together in order to ensure that there is the maximum protection so that there can be the maximum use. And if we do that, I think we will continue to lead the world and improve the quality of life in this country dramatically.

But to the extent that there continues to be a residue of mistrust and an unwillingness to work together, it inhibits this wonderful opportunity that we have.

Actually, there is one last question I would like to ask both of you because I think it is important for particularly our viewers and people who came to this hearing to appreciate. If you want to know more about how to make your own systems secure, let's say you are a small business here in Arizona, what is the best advice you have to individuals or small businesses? I am sure big businesses have found their way to your doorstep, but how does a small business do the best it can in an economic way to provide the security that it needs?

Mr. GRANADO. There are a lot of organizations that folks and small businesses can join—Information Systems Security Organization is just one—where members of small businesses can join these organizations, and they have monthly meetings of security professionals within that specific community to discuss vulnerability issues, strategic issues, tactical issues with respect to systems security. So that would be one good economic avenue to gain knowledge on this issue.

Then the other point, again, what I alluded to earlier, the Internet is just full of information that is free and easily accessible. You know, I described today the hacking-related information. There is just as much information out there on how to secure your system, and step by step how to secure it, that people can just do searches on the Internet, pull that information, pull out what is specific to their machines, and work on securing their systems, again, free and all that is required is Internet access.

Mr. AUCSMITH. And that is the nice thing about the Internet, its opportunities. There are bad guys out there, but there are also good guys. You can find lists of places to go for the good guys. There is a variety of sources for finding that, just a general search will probably help, but you can start with CERT, which is an organization at Carnegie Mellon. The Computer Emergency Response Team has a wide range of links that you can go to where the good guys are. The problem with all of that is it is necessary to have the technical competence to make that a reality in small business, and many small businesses lack that resource, in which case, much as you might call a locksmith or a burglar alarm company to help protect your physical security, you may very well need to make the investment of contacting a security professional to help you with your cyber security.

Senator KYL. And probably one of the most important points is, even though you develop what you think is a secure system, always understand that there are numerous vulnerabilities, and you have got to constantly be alert to the little things, you know, leaving your password taped to the top of your computer, as I saw one time, by the way—I mean, it sounds silly, but there are a lot of vulnerabilities that people just don't stop to think, basically, about what they need to do to make their systems secure.

Mr. AUCSMITH. We put them underneath the keyboards.

Senator KYL. Yes, right. [Laughter.]

That is a good metaphor for the need to always be alert that there could be a problem, even though you have secured what you think is a pretty good system. But the first step is to try to take advantage of this.

I am informed and we learned at our hearing in Washington that this Carnegie Mellon entity which Mr. Aucsmith alluded to had developed good counter-software to the kind of denial-of-service attack that occurred against some of the sites that we have been referring to today. Some entities took advantage of that software. Some did not. Those that did didn't experience that denial of service.

So take advantage of that which is available to you as has been described and remain alert to the possibility that even that won't

necessarily deter a determined hacker. I guess those would be the two watch words.

I really appreciate your demonstration, Mr. Granado, and, Mr. Aucsmith, your expertise in this. I will hope to continue to plumb the depths of that expertise as we try to fashion the kind of national policy and legislative solution to develop this cooperation that is going to be so essential to the future, and I look forward to continuing to cooperate with you.

I thank all of you who have joined us at this hearing today. As I said at the beginning, this is an official hearing of the U.S. Senate Judiciary Committee's subcommittee which I chair, and anyone who wishes to communicate with us, we can put your comments in the record if they are appropriate. If you have questions, obviously submit them through me, and perhaps we will have an opportunity to share those with our witnesses here today.

If there is nothing further, then I will declare this meeting adjourned.

[Whereupon, at 10:30 a.m., the subcommittee was adjourned.]

○