COMPUTER SECURITY: CYBER ATTACKS—WAR WITHOUT BORDERS

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JULY 26, 2000

Serial No. 106–252

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE
74–152 DTP WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. McINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LaTOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH-HAGE, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

BERNARD SANDERS, Vermont (Independent)

Kevin Binger, *Staff Director*
Daniel R. Moll, *Deputy Staff Director*
James C. Wilson, *Chief Counsel*
Robert A. Briggs, *Clerk*
Phil Schiliro, *Minority Staff Director*

Subcommittee on Government Management, Information, and Technology

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

Ex Officio

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. Russell George, *Staff Director and Chief Counsel*
Bonnie Heald, *Director of Communications*
Bryan Sisk, *Clerk*
Trey Henderson, *Minority Counsel*

CONTENTS

COMPUTER SECURITY: CYBER ATTACKS—WAR WITHOUT BORDERS

WEDNESDAY, JULY 26, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:02 a.m., in room 2157, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Davis, Turner, and Maloney.

Also present: Tatjana Antonova, Latvian interpreter.

Staff present: J. Russell George, staff director and chief counsel; Ben Ritt, GAO detailee; Bonnie Heald, director of communications; Bryan Sisk, clerk; Elizabeth Seong, staff assistant; Will Ackerly and Davidson Hulfish, interns; Trey Henderson, minority counsel; and Jean Gosa, minority clerk.

Mr. HORN. A quorum being present, the hearing of the House Subcommittee on Government Management, Information, and Technology will come to order.

I apologize for being a little late. It's the first time it has happened, but we had a party conference this morning and we got a new Member, so that takes a little time. That is Mr. Marty Martinez, who switched parties to come with us because he wanted common sense government.

From the "ILOVEYOU" virus to attempts to enter the space shuttle's communication system, cyber attacks are on the rise. Every day new viruses and attempted intrusions bombard vital computer systems and networks within U.S. Government agencies and private industries. Sometimes the attackers are simply seeking the thrill of breaking into a supposedly secure system. Other times, however, the motive is far more sinister—vandalism, industrial espionage, intelligence collection, or creating a doorway for a future attack. As the "ILOVEYOU" virus clearly demonstrated, these attacks can originate from nearly anywhere in the world.

Many experts say this is only the tip of the iceberg in terms of the number of attacks, their sophistication and their destructiveness. In the United States and in many other countries, law enforcement agencies and private organizations collect and share information on these worldwide computer attacks. However, not all countries have the capability to detect them, warn others, or even prosecute the hackers once they have been identified.

In the United States, the Federal Bureau of Investigation and the Departments of Commerce and Defense all have a role in tracking and investigating cyber attacks. Many other agencies and private organizations also track and share this critical information. Other countries also have law enforcement agencies and organizations set up to investigate and share cyber attack information. But among the variety of players, who is coordinating an efficient, effective response to this international problem?

Today, we will examine the challenges of coordinating these cyber attack investigations. Our witnesses represent cyber crime investigation units in several countries, including the United States. They will discuss their experiences. There is a great need for a sharing of these experiences daily, weekly and at least monthly. Alliances such as the North Atlantic Treaty Organization should work together if we will be able to win these cyber wars.

We welcome each of our witnesses. We appreciate many of you that have taken a long journey to come here, and we look forward to the testimony you will submit, and it will be put through the processes to go to the full House of Representatives after this and other hearings have come by.

So we will now turn to the ranking member, the gentleman from Texas, Mr. Turner, for an opening statement.

[The prepared statement of Hon. Stephen Horn follows:]

AN BURTON, INDIANA,
CHAIRMAN

ENJAMIN A. GILMAN, NEW YORK
ONSTANCE A. MORELLA, MARYLAND
HRISTOPHER SHAYS, CONNECTICUT
EANA ROS-LEHTINEN, FLORIDA
OHN M. McHUGH, NEW YORK
TEPHEN HORN, CALIFORNIA
OHN L. MICA, FLORIDA
HOMAS M. DAVIS III, VIRGINIA
AVID M. McINTOSH, INDIANA
ARK E. SOUDER, INDIANA
OE SCARBOROUGH, FLORIDA
TEVEN C. LaTOURETTE, OHIO
ARSHALL "MARK" SANFORD, SOUTH CAROLINA
OB BARR, GEORGIA
AN MILLER, FLORIDA
SA HUTCHINSON, ARKANSAS
EE TERRY, NEBRASKA
UDY BIGGERT, ILLINOIS
REG WALDEN, OREGON
OUG OSE, CALIFORNIA
AUL RYAN, WISCONSIN
OHN T. DOOLITTLE, CALIFORNIA
ELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS

Congreſs of the United States

Houſe of Repreſentatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY	(202) 225–5074
MINORITY	(202) 225–5051
TTY	(202) 225–6852

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
GARY A. CONDIT, CALIFORNIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, JR., TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

Computer Security:
"Cyber Attacks -- A War without Borders"

Opening Statement
Chairman Stephen Horn (R-CA)
Subcommittee on Government Management,
Information, and Technology
July 26, 2000

A quorum being present, the hearing of the House Subcommittee on Government Management, Information, and Technology will come to order.

From the "ILOVEYOU" virus to attempts to enter the space shuttle's communications system, cyber attacks are on the rise. Every day, new viruses and attempted intrusions bombard vital computer systems and networks within U.S. Government agencies and private industries.

Sometimes the attackers are simply seeking the thrill of breaking into a supposedly secure system. Other times, however, the motive is far more sinister -- vandalism, industrial espionage, intelligence collection, or creating a doorway for a future attack. As the "ILOVEYOU" virus clearly demonstrated, these attacks can originate from nearly anywhere in the world.

Many experts say this is only the tip of the iceberg in terms of the number of attacks, their sophistication, and their destructiveness. In the United States, and in many other countries, law enforcement agencies and private organizations collect and share information on these worldwide computer attacks. However, not all countries have the capability to detect them, warn others, or even prosecute the hackers once they have been identified.

In the United States, the FBI and the Departments of Commerce and Defense all have a role in tracking and investigating cyber attacks. Many other agencies and private organizations also track and share this critical information. Other countries also have law enforcement agencies and organizations set up to investigate and share cyber-attack information. But among the myriad players, who is coordinating an efficient, effective response to this international problem?

Today, we will examine the challenges of coordinating these cyber-attack investigations. Our witnesses represent cyber-crime investigation units in several countries, including the United States, who will discuss their experiences.

We welcome each of our witnesses, and look forward to their testimony.

Mr. TURNER. Thank you, Mr. Chairman. We know that the United States and many industrialized nations now depend on the interconnected computer system that we call the Internet. We know that it supports critical operations in the private sector as well as government. And we understand that the increased reliance upon the Internet has caused us to be highly vulnerable to cyber attacks.

These cyber attacks know no boundaries and can occur from anywhere in the world. I had the opportunity to visit with some members of the European Parliament a few weeks ago and it came home to me how much we have in common in terms of trying to deal with the new systems that are in place upon which we all know we depend for our very livelihood.

It is important for law enforcement agencies throughout the world to work cooperatively in the defense against those who would perpetuate computer crimes. And in order to more effectively fight this battle, we need to coordinate our information sharing and cooperate as an international community to be sure that we are protecting our citizens and our livelihoods.

This committee has had three hearings now on this subject and many of you on the panel today have traveled long distances to come and share your thoughts with us, for which we are extremely appreciative and grateful. I look forward to hearing from each of you, and I hope that this can be a part of our continuing effort to work nation to nation to ensure that we can defend against cyber attacks and protect the security of our systems.

Thank you, Mr. Chairman.

[The prepared statements of Hon. Jim Turner and Hon. Thomas M. Davis follow:]

STATEMENT OF THE HONORABLE JIM TURNER
GMIT: "Computer Security: Cyber Attacks - War Without Borders"
7/26/00

Thank you, Mr. Chairman. More than any other nation, the United States depends on interconnected computer systems -- including the Internet -- to support critical operations and services both in the public and private sectors. While beneficial, this increased reliance on digital services has left us highly vulnerable to cyber-attacks. The federal government recognizes the significance of these threats, and a number of federal agencies have been charged with protecting our computer systems. However, cyber-attacks know no boundaries and can occur from anywhere in the world. Therefore, law enforcement agencies in other countries, as well as Interpol, are also important part of our defense against those who seek perpetrate computer crimes. In order to most effectively fight the battle against cyber-attacks, we need to coordinate information sharing and cooperation in the international community.

This is the Subcommittee's third hearing on this subject, and I commend the Chairman for his focus on this critical issue. I welcome the witnesses who represent cyber-crime investigation units who have agreed to share their experiences and the challenges they face in coordinating cyber-attack investigations. I know many of you have a come along way to be with us this morning. Hopefully, this hearing and the work of the Subcommittee will lead to a continuing effort of sharing and cooperation among all stakeholders on this issue.

Statement of Representative Tom Davis
Subcommittee on Government Management, Information, and Technology
Oversight Hearing on Computer Security: "Cyber Attacks—
A War Without Borders"
July 26, 2000

Mr. Chairman, I greatly appreciate your leadership in bringing the critical issue of computer security and its global implications to the forefront of this Subcommittee's consideration. Since early March, we have examined a number of aspects of security in the cyber world. We first focused on the state of our nation's readiness in the face of cyber attacks on both the Federal Government and the private sector and then moved to the tools being utilized to prevent and reduce intrusions. And last month, in discussing legislation I introduced with Congressman Jim Moran, the Cyber Security Information Act of 2000, the Subcommittee examined the importance of public-private partnerships for strengthening computer security and reducing the vulnerabilities of information systems that operate and connect our nation's critical infrastructure.

This hearing is the next fundamental step in learning how Federal agencies can work both together and with their overseas counterparts to build effective international cooperation on cyber security. As we are all aware, the Internet is rapidly becoming the central backbone of our global economy and our international communications network. While we must address the protection of our national systems, it is manifest that without understanding the evolution and operation of cyber attacks from a worldwide perspective, we will never be able to effectively deflect assaults that can originate from far-flung corners of the globe without an international cyber security strategy.

With the near doubling of Internet security incidents in the first half of this year as compared to all of last year, the urgency of this problem has been intensified by the explosive growth of the Internet as a primary means of national and international commerce. A June 6th report issued by the University of Texas found that the Internet Economy grew to $523.9 billion in 1999 and estimated its growth at $850 billion in 2000. That same study noted that Internet-related revenue growth was 15 times the growth rate for the U.S. economy last year. But the prosperity that is increasingly supporting the health and quality of life in our communities, and the medium that allows friends and family across the world to maintain close ties, faces increased security threats. Although many of the attacks we have experienced so far have been generated mainly by thrill seekers, the tools for wreaking havoc throughout the Internet are easily available. We need to prepare our governments and our citizens for more hostile perpetrators, as well as prevent the less malicious intrusions from disrupting the Internet's crucial role in our daily economic and social lives.

Figuring out how the Federal Government can work with other nations to share information and coordinate investigations of cyber attacks is an essential component of our inquiry here today. We know from our previous hearings that control over the United States' critical infrastructure lies almost entirely with the private sector, and that these assets are linked together through computers and computer networks. As the title of our

Page 3 of 3

hearing describes, the Internet is indeed the cyber conduit that makes America's critical infrastructure vulnerable to threats from anywhere around the world. For these reasons, I am particularly interested in hearing from our international witnesses about the makeup and ownership of critical infrastructure within their own economies, and any efforts they have made to encourage information sharing within their borders as well as outside of them. I look forward to hearing the testimony of each of our witnesses today, and to gathering their expertise for coordinating the detection and investigation of cyber attacks within the international community.

Mr. HORN. We thank you very much for all you have done to pursue some of these real questions and we appreciate that.

We are now turning to the witnesses. We are notified that we might have to recess for the first vote of the day, and that is one of the problems we have when we are in the middle of a hearing where we would rather keep going. Our duty is to get over to the floor and get back. So that might happen around 10:30. So I would like to begin with this panel.

The way this operation works with all presentations, since it is an investigating committee, is that we swear all the witnesses in on a truth oath. And we will call—when we call on you based on the agenda, the full written statement of yours and the resume goes into the record so we don't have to hear the paper you gave us read. We like you to summarize it because that way it permits a dialog within the panel as well as the Members who will be here.

So we do not want you to really read your work; just summarize it for us. We will now ask to you stand and raise your right hands.

[Witnesses sworn.]

Mr. HORN. The clerk will note that all the witnesses have taken the oath.

We start with Mr. Michael Vatis, the Director, National Infrastructure Protection Center of the Federal Bureau of Investigation. Mr. Vatis.

STATEMENTS OF MICHAEL VATIS, DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION; JURIS REKSNA, CHIEF OF STATE POLICE, MINISTRY OF INTERNAL AFFAIRS, LATVIA; STEFAN KRONQVIST, CHIEF, COMPUTER CRIME UNIT, NATIONAL CRIME INVESTIGATION DEPARTMENT, SWEDEN; JUERGEN MAURER, DETECTIVE CHIEF SUPERINTENDENT, GERMAN FEDERAL POLICE OFFICE; ELFREN L. MENESES, JR., ANTIFRAUD AND COMPUTER CRIMES DIVISION, NATIONAL BUREAU OF INVESTIGATION, PHILIPPINES; OHAD GENIS, ADVOCATE, CHIEF INSPECTOR, NATIONAL UNIT FOR FRAUD INVESTIGATIONS, ISRAEL POLICE; AND EDGAR A. ADAMSON, CHIEF, U.S. NATIONAL CENTRAL BUREAU—INTERPOL

Mr. VATIS. Thank you, Mr. Chairman, Congressman Turner; I very much appreciate the opportunity to testify before you today, particularly in the presence of so many of my international colleagues. I am not aware of any previous hearing that has had so many international law enforcement officials together in one place, especially on an issue where international cooperation is so vital to our success. So I applaud the committee for holding this hearing in this manner.

As you know, the National Infrastructure Protection Center was set up in February 1998 and authorized by Presidential Decision Directive 63 to serve as the government's focal point for collecting information about cyber threats and attacks, analyzing that information, issuing pertinent warnings to both government agencies and private industry, and also coordinating the government's response to attacks that do occur.

That mission requires cooperative arrangements with a variety of entities, both governmental and in the private sector. We need to have close relationships with other Federal agencies, with State and local law enforcement, with the private sector owners and operators of the Nation's critical infrastructures and, most pertinent to this hearing, with our foreign law enforcement counterparts, and we try to achieve those cooperative arrangements through a variety of mechanisms.

With other Federal agencies, the first mechanism is by having those agencies represented in the NIPC, which is, while located at FBI, an interagency center. So we have numerous representatives from various components of the Department of Defense, from the Intelligence Community, from the Department of Commerce, and from other agencies as well.

We also have State and local law enforcement representation, as well as foreign liaison representation. That interagency composition allows us to coordinate more effectively when there is an incident or when there is the requirement to share information across agencies and with the private sector as well.

We also reach out to the private industry through a variety of outreach initiatives, including our InfraGard program, which is an initiative to share information about incidents in a two-way fashion, both so industry can share information with us that they become aware of and so we can share information with them about incidents that we become aware of through law enforcement or intelligence means.

In addition, we reach out to our private industry counterparts through various conferences and outreach initiatives to try to generate awareness and to convince them of the need to raise security in general, because even with all of our warning efforts, if we do not have better security there is no way we can really make headway against this problem. The situation right now is such that vulnerabilities are so rampant throughout the Internet that until the bar is raised against attacks, all of the government's efforts really would be wasted. So we are trying to work in tandem with the private sector to encourage it to raise the level of security while also improving our ability in the government to respond to attacks and issue warnings effectively.

Finally, with regard to foreign law enforcement, I think it is commonly understood now that in the area of cyber crime, foreign cooperation is absolutely critical because the Internet knows no boundaries. It is as easy to launch an attack from a foreign country as it is from within the United States. And as a result, we are increasingly finding that our investigations lead us to foreign countries, where we have to seek the assistance and cooperation of the domestic law enforcement agency because we don't have the authority or the capability to conduct searches or witness interviews or electronic surveillances in a foreign country. So international cooperation is absolutely critical.

We have had a number of cases over the last 2 years which have demonstrated, I think, a great improvement in our ability to coordinate with foreign countries. In 1998, we had the Solar Sunrise incident, which involved wide scale intrusions into Department of Defense computer networks. We tracked down the intruders with the assistance of the Israeli National Police and identified two juveniles in the United States and several individuals in Israel who were responsible for those intrusions.

This year, we had the arrest of an individual in the United Kingdom who had broken into Web sites and stolen credit card numbers and posted many of those numbers on a Web site. That case was successfully resolved because of close cooperation between the FBI and a local Welsh police service.

We also had most notably the denial of service attacks in February of this year—many of those attacks have been attributed to a juvenile in Canada—based in large part on very close working relationships between the FBI and the Royal Canadian Mounted Police.

And then finally we had the "Love Bug," or "ILOVEYOU" virus in May of this year. And in that case too, a suspect was identified in the Philippines really with unprecedented speed, based again on the very close working relationship between the FBI and the Philippines National Bureau of Investigation.

So I think all of those major successes demonstrate that we have made a great deal of progress in improving coordination with foreign law enforcement agencies. There is clearly a long way to go because there are so many countries in the world, and as we see the Internet continue to expand we're not going to need cooperation just from our close allies within the G–8 or within European countries and our traditional allies in Asia, but we are going to need more cooperation from countries that we have not traditionally worked together with, and that will pose even more challenges as we try to continue to expand our network of contacts.

So I look forward to answering any questions that you have, but I think that sums up the situation from the U.S. perspective.

[The prepared statement of Mr. Vatis follows:]

Statement of Michael A. Vatis
Director
National Infrastructure Protection Center
Federal Bureau of Investigation
before the
House Committee on Government Affairs
Subcommittee on Government Management, Information, and Technology

July 26, 2000

Good morning, Chairman Horn, Congressman Turner, members of the subcommittee, and distinguished guests. I am pleased to testify before this subcommittee today on our international response to cyber attacks and computer crime in general. The representation you have assembled for this hearing is truly extraordinary. To my knowledge, never have so many international law enforcement officials testified before Congress at one time on issues related to cyber intrusions and computer crime. A recently released study estimates that computer viruses and hacking take a toll of $1.6 trillion on the global economy.[1] This figure dwarfs the gross national product of most of the world's nations. Given the global nature of the computer crime problem and the fact that many of our investigations in the U.S. have an international nexus, it is vital that we work effectively across borders in concert with our international partners. I believe this hearing will contribute to that effort and highlight the extensive endeavors we have already made in the international arena.

Protecting the Nation's critical infrastructures and combating computer intrusions is by necessity a cooperative effort. National governments must work within themselves, across agencies; with regional and local law enforcement; with private industry; and with foreign governments to combat the problem. If cooperation is lacking in any one of these areas, the whole effort will fall short. Yet if cooperation is effective across all of these areas, then we can gain the upper hand against cyber criminals around the world and ensure that the Internet is a safe place for electronic commerce and communication.

Cooperative Structures in the United States

The U.S. government approach to protecting the nation's critical infrastructures is outlined in Presidential Decision Directive (PDD) 63, issued in May 1998. That Directive forms a series of cooperative arrangements. In particular, PDD-63 categorizes our infrastructures into

[1] PR Newswire article, July 7, 2000. See **http://news.excite.com/news/pr/000707/ny-study-viruses.**

several sectors and designates federal "Lead Agencies,"[2] which are responsible for working cooperatively with private industry from each sector to develop mechanisms and plans for securing that sector against cyber attacks and for recovering should an attack occur.

The PDD also gives a significant coordinating role for operational matters to the National Infrastructure Protection Center (NIPC), which I head. The PDD places the NIPC at the core of the government's warning, investigation, and response system for threats to, or attacks on, the nation's critical infrastructures. The NIPC is the focal point for gathering information on threats to the infrastructures as well as "facilitating and coordinating the Federal Government's response to an incident." The PDD further specifies that the NIPC should include "elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach, and development and application of technical tools."

The NIPC has a vital role in collecting and disseminating information from all relevant sources. The PDD directs the NIPC to "sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state, and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity." The NIPC is also charged with issuing "attack warnings or alerts" to the owners and operators of critical infrastructures in the private sector.

In order to perform its role, the NIPC has established, and is continuing to expand, a network of cooperative relationships with a wide range of entities in both the government and the private sector. First, the Center, while located at the FBI, is interagency in its composition, bringing together representatives from the law enforcement, defense, and intelligence communities, as well as from many of the lead agencies specified in the PDD. The Center currently has representatives from the following federal entities: Navy, Air Force, Army, Air Force Office of Special Investigations, Naval Criminal Investigative Service, Defense Security Service, National Security Agency, United States Postal Service, Federal Aviation

[2] The Lead Agencies are: Commerce for information and communications; Energy for Electric Power as well as oil and gas production and storage; Treasury for banking and finance; EPA for water supply; Transportation for aviation, highways, mass transit, pipelines, rail, and waterborne commerce; Justice/FBI for emergency law enforcement services; Federal Emergency Management Agency for emergency fire service and continuity of government; Health and Human Services for public health services. The Lead Agencies for special functions are: State for foreign affairs, CIA for intelligence, Defense for national defense, and Justice/FBI for law enforcement and internal security. The NIPC performs the lead agency and special functions roles specified for "Justice/FBI" in the PDD.

Administration, General Services Administration, Central Intelligence Agency, Critical Infrastructure Assurance Office, and Sandia National Laboratory. In addition, the Center has had state law enforcement officials detailed on a rotating basis. So far we have had representatives from the Oregon State Police and the Tuscaloosa County (Alabama) Sheriff's Department. We also have international liaison officials who work with the Center. This interagency composition facilitates the NIPC's ability to share pertinent information among agencies and to coordinate agencies' activities in the event of an attack.

Second, pursuant to the PDD, the NIPC has electronic links to the rest of the government in order to facilitate the sharing of information and the issuance of warnings. Third, the PDD directs all executive departments and agencies to "share with the NIPC information about threats and warning of attacks and actual attacks on critical government and private sector infrastructures, to the extent permitted by law." Fourth, to bolster our technical capabilities the Center selectively employs private sector contractors. By bringing other agencies directly into the Center and building direct communication linkages to government agencies and the private sector, the Center provides a means of coordinating the government's cyber expertise and ensuring full sharing of information, consistent with applicable laws and regulations.

In addition, in its role under Presidential Decision Directive (PDD) 63 as the lead agency for the "Emergency Law Enforcement Sector" (ELES), the NIPC has been working with state and local law enforcement to develop a plan to protect that sector from cyber attack and reduce its vulnerabilities. As part of that effort, the NIPC's alerts and warnings are regularly sent to state and local law enforcement agencies via the National Law Enforcement Telecommunications System (NLETS) and through NIPC e-mail via the Law Enforcement Online system. Sharing with state and local law enforcement is critical because they are often the first responders when an incident occurs.

To fulfill its mandate under PDD-63, the NIPC's goal is to develop a comprehensive "indications and warning" system that will be capable of timely collection of indicators of an imminent or ongoing cyber attack, analysis of the information, and the timely issuance of alerts and warnings. This will require additional resources, both personnel and equipment. It will also require participation by the Intelligence Community; the Department of Defense; the sector "Lead Agencies"; other government agencies; federal, state and local law enforcement; and the private sector owners and operators of the infrastructures. As I will discuss further in a moment, the NIPC is currently working with industry to develop a methodology and system for detecting and warning of attacks on the national telecommunications and electric power sectors. These will provide a model for possible systems for the other sectors.

Finally, the NIPC, as the national entity responsible for government's warning, investigation, and response system for threats to, or attacks on, the nation's critical infrastructures, works on national planning initiatives with the National Security Council and the Critical Infrastructure Assurance Office.

To accomplish its goals under the PDD, the NIPC is organized into three sections:

- The Computer Investigations and Operations Section (CIOS) is the operational and response arm of the Center. It program manages computer intrusion investigations conducted by FBI Field Offices and some of the joint task forces throughout the country; provides subject matter experts, equipment, and technical support to cyber investigators in federal, state, and local government agencies involved in critical infrastructure protection; and provides a cyber emergency response capability to help resolve a cyber incident.

- The Analysis and Warning Section (AWS) serves as the "indications and warning" arm of the NIPC. The AWS reviews numerous government and private sector databases, media, and other sources daily to collect and disseminate information that is relevant to any aspect of NIPC's mission, including the gathering of indications of a possible attack. It provides analytical support during computer intrusion investigations, performs analyses of infrastructure risks and threat trends, and produces current analytic products for the national security and law enforcement communities, the owners-operators of the critical infrastructures, and the computer network managers who protect their systems. It also distributes tactical warnings, alerts, and advisories to all the relevant partners, informing them of exploited vulnerabilities and threats.

- The Training, Outreach and Strategy Section (TOSS) coordinates the training and continuing education of cyber investigators within the FBI Field Offices and other federal, state and local law enforcement agencies. It also coordinates our liaison with private sector companies, state and local governments, other government agencies, and the FBI's Field Offices. In addition, this section manages our collection and cataloguing of information concerning "key assets" -- i.e., critical individual components within each infrastructure sector, such as specific power facilities, telecommunications switch nodes, or financial systems -- across the country.

To facilitate our ability to investigate and respond to attacks, the FBI has created the National Infrastructure Protection and Computer Intrusion (NIPCI) Program in the 56 FBI Field Offices across the country. We currently have 193 agents nationwide dedicated to investigating computer intrusion, denial of service, and virus cases (less than 2% of all FBI agents nationwide). In order to leverage these resources most efficiently, we have taken the approach of creating 16 regional squads that have sufficient size to work complex intrusion cases and to assist those field offices without a full NIPCI squad. In those field offices without squads, the FBI has established a baseline capability by having at least one or two agents to work NIPCI matters, i.e. computer intrusions (criminal and national security), viruses, the InfraGard and Key Asset Initiatives, and state and local liaison.

In addressing cyber incidents, the NIPC and the 56 FBI field offices work cooperatively with their federal, state and local law enforcement partners and with the private sector. For example, in the Melissa Macro Virus investigation, the NIPC issued public warnings that helped alert the public, government agencies, and private industry to the virus and stem the damage to computer networks. In addition, the FBI's Newark office worked closely with the New Jersey State Police, the New Jersey Attorney General's Office, and the U.S. Attorney's Office in New Jersey in the investigation, arrest, and prosecution of David L. Smith. The NIPC supported the overall investigation which spanned the nation. In other cases where there is concurrent jurisdiction, the FBI and other agencies often work cases jointly. For example, the FBI and the U.S. Secret Service worked together on a series of hacks into the White House Homepage. Eric Burns, a.k.a Zyklon, hacked into the White House web site as well as other sites. He was caught and pled guilty to one count of 18 U.S.C.1030. In November 1999 he was sentenced to 15 months in prison, 3 years supervised release, and ordered to pay $36,240 in restitution and a $100 fine. While I cannot discuss it in open hearings, the NIPC also works closely with other agencies in foreign counter intelligence investigations involving cyber attacks.

Government-Industry Cooperation

As I noted earlier, however, it is critical for the government not just to work cooperatively within itself, but also with the private sector. The NIPC is engaged in several initiatives to work cooperatively with the private sector, principally in the area of information sharing. First, the NIPC, in conjunction with the private sector, has developed an initiative call "InfraGard" to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and infrastructure threats. The initiative encourages and facilitates the exchange of information by government and private sector members through the formation of local InfraGard chapters within the jurisdiction of each FBI Field Office. Chapter membership includes representatives from the FBI, private industry, other government agencies, state and local law enforcement, and the academic community. The critical component of InfraGard is the ability of industry to provide information on intrusions to the NIPC and to the local FBI Field Office, using secure communications, in both a "sanitized" and detailed format. The local FBI Field Offices can, if appropriate, use the detailed version to initiate an investigation; the NIPC, in turn, can analyze that information in conjunction with other law enforcement, intelligence, and industry information to determine if the intrusion is part of a broader attack on numerous sites. The Center can simultaneously use the sanitized version to inform other members of the threat and the techniques used, without compromising the confidentiality of the reporting company. The secure website also contains a variety of analytic and warning products that we make available to the InfraGard community.

We believe InfraGard, once fully implemented, will be a significant step forward in enhancing the ability of the private sector and the government to share information with each other. The government has access to unique sources of information through its intelligence and law enforcement activities. These need to be shared, in appropriately sanitized form, with private sector owners and operators so that they can protect themselves against threats that we become aware of. Conversely, the private sector is often the victim of cyber attacks and threats that are highly relevant to our mission to protect that nation's critical infrastructures from attack. Only by bringing these governmental and private sources of information together can we get a sense of the full picture of threats and incidents, draw linkages, and engage in effective "indications and warning" regarding cyber attacks. In contrast to efforts to share information solely within one industry sector, InfraGard provides a vehicle for sharing information across sectors and between the government and industry generally.

A second effort involving cooperation with the private sector is the Key Asset Initiative (KAI). A key asset can be defined as an organization, system, group of organizations or systems, or physical plant, the loss of which would have widespread and dire economic or social impact on a national, regional, or local basis. The KAI initially 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 case of an emergency. Eventually, contingent on future funding, the KAI 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 Center maintains a national database. This initiative serves the critical needs of developing lists of the key assets within each critical infrastructure and also of developing the communications and liaison links necessary for the collection of information and the dissemination of warnings to the infrastructure owners and operators.

Another initiative is a pilot program we have developed with the North American Electrical Reliability Council (NERC) to develop an "Indications and Warning" System for physical and cyber attacks. Under the pilot program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the pilot program have stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. NERC has recently decided to expand this initiative nationwide. We see this initiative as a good example of government and industry working together to share information and it is our expectation that the Electrical Power Indications and Warning System will provide a model for the other critical infrastructures. We are currently working with industry on developing an Indications and Warning program for the telecommunications sector.

The NIPC has also been working on a set of outreach conferences under the auspices of the Department of Justice and the Information Technology Association of America. In April, 2000 the Attorney General, representatives from the NIPC, Special Agents from FBI Field Offices, and other law enforcement officials met with west coast industry representatives at Stanford University. Last month, we met with east coast industry representatives at EDS in Herndon, Virginia. At both conferences the Attorney General stressed ways that industry and law enforcement need to work together against computer hackers and intrusions. It was clear at both conferences, too, that industry wants a good, cooperative relationship with law enforcement to share information about threats and incidents, and to investigate cyber attacks successfully. A number of initiatives stemming from those conferences are currently underway to further this cooperative relationship.

NIPC representatives spend a significant portion of our time speaking across the country and around the world to private sector and government groups, as part of our effort to raise awareness about the cyber threat and to foster cooperation between industry and law enforcement. For example, we have recently participated in meetings of the National Security Telecommunications Advisory Committee (NSTAC), a private sector advisory committee to the President whose purpose is to provide advice and expertise on national security and emergency preparedness telecommunications policy); the System Administration, Networking, and Security (SANS) Institute, a cooperative research and education organization founded in 1989 for the purpose of sharing information among system administrators, security professionals, and network administrators; the Information Security Forum, an association of organizations who share best practices and other solutions to information security problems; the National Governors Association; the American Society for Industrial Security (ASIS), a 32,000 member organization for professionals responsible for security; and the American Bar Association (ABA).

Finally, the NIPC is working with the Critical Infrastructure Assurance Office in the Department of Commerce on outreach initiatives. All of these efforts are critical to the goal of building a partnership between industry and the government for the purpose of securing our nation's critical infrastructures and reducing our vulnerability to cyber crime.

NIPC and International Cooperation

Most pertinent to this hearing is the issue of cooperation across national borders. A typical cyber investigation can involve victim sites in multiple states and often many countries, and can require tracing an evidentiary trail that crosses numerous state and international boundaries. Even intrusions into U.S. systems by a perpetrator operating within the U.S. often require international investigative activity because the attack is routed through Internet Service

Providers and computer networks located outside the United States. When evidence is located within the United States, we can subpoena records, conduct electronic surveillance, execute search warrants, seize evidence, and examine it. We can do none of those things ourselves overseas to solve a U.S. criminal case. Instead, we must depend on the local authorities to assist us. This means that effective international cooperation is essential to our ability to investigate cyber crime.

International investigations pose special problems. First, while the situation has improved markedly in recent years, many countries lack substantive laws that specifically criminalize computer crimes. This means that those countries often lack the authority not only to investigate or prosecute computer crimes that occur within their borders, but also to assist us when evidence might be located in those countries. Moreover, the quickly evolving technological aspects of these investigations can exceed the capabilities of local police forces in some countries. Finally, even when countries have the requisite laws and have developed the technical expertise necessary to conduct cyber investigations, successful investigation in this arena requires more expeditious response than has traditionally been the case in international matters, because electronic evidence is fleeting and, if not secured quickly, can be lost forever.

NIPC International Outreach

The NIPC is working with its international partners on several fronts to address the issues outlined above. The first area consists of outreach activities designed to raise awareness about the cyber threat, encourage countries to address the threat through substantive legislation, and provide advice on how to organize to deal with the threat most effectively. Almost weekly the NIPC hosts a foreign delegation to discuss topics ranging from current cases to the establishment of NIPC-like entities in other nations. Since the NIPC was founded, Japan, the United Kingdom, Canada, Germany, and Sweden have formed or are in the process of forming interagency entities like the NIPC. The NIPC has briefed visitors from the United Kingdom, Germany, France, Norway, Canada, Japan, Denmark, Sweden, Israel, and other nations over the past year. In addition, to promote understanding of the NIPC mission, an "open house" for embassy personnel was held in March 2000.

Abroad, the FBI's Legal Attaches (Legats) are often the first officials contacted by foreign law enforcement should an incident occur. We are providing training to our Legats on how to coordinate computer intrusion and infrastructure protection matters with us to make them more effective. In addition, NIPC personnel are in almost daily contact with Legats around the world to assist in coordinating requests for information.

NIPC International Training

In order to help make our foreign partners more capable to assist our international investigations and to address cyber crime within their own countries, the NIPC has also provided training to investigators from several nations. Much of this training takes place at the International Law Enforcement Academies in Budapest, Hungary and Bankok, Thailand. In addition, a small number of select international investigators receive training in NIPC sponsored classes in the United States. The NIPC also holds workshops with other nations to share information on techniques and trends in cyber intrusions. For example, in September 1999 the NIPC sponsored an International Cyber Crime Conference in New Orleans to provide training to international law enforcement officers and forge links between foreign law enforcement officers and personnel representing: the NIPC, FBI field offices, FBI Legats, the U.S. Secret Service, the Naval Criminal Investigative Service, the Air Force Office of Special Investigations, and the U.S. Postal Inspection Service.

The G-8 High-Tech Crime Working Group

Another international initiative that the NIPC has been involved in is the G-8's High-Tech Crime Subgroup of the G-8 "Lyon Group." A representative of the NIPC serves as a member of the United States delegation to the Subgroup, which has been considering several issues concerning international cyber crime investigations, including the establishment of a 24/7 high-tech crime points of contact network, international training conferences, review of legal systems in G-8 countries, and the development of the G-8 principles on transborder access to stored computer data.

The 24/7 high-tech points of contact network was established in March 1998. Each of the G-8 countries identified a point of contact for law enforcement in each of their respective countries. These contacts are required to be available twenty-four hours a day, seven days a week, in order to respond to requests for assistance in important high-tech crime investigations in which electronic evidence may either be altered or destroyed.

With regard to training, the subgroup hosted an international computer crime training conference in November 1998, for law enforcement investigators of the G-8 countries. This conference addressed law enforcement issues relating to high-tech crime investigations and the technical issues involved in these specific types of investigations. In addition, the subgroup has compiled a collection of the substantive and procedural laws regarding computer crimes in each of the G-8 countries. Regarding the critical issue of transborder access to stored data, the subgroup has provided recommendations for principles of transborder access to stored computer data. In addition, the subgroup has written principles that provide a mechanism to secure the rapid preservation of stored data in computer systems. These recommendations will attempt to prevent instances where computer data of possible evidentiary value is altered or deleted while a formal request for assistance under a Mutual Legal Assistance Treaty (MLAT) is processed. Lastly, the G-8 subgroup has referred the task of developing common terms and common formats for forensic requests and developing international standards for the retrieval and processing of electronic evidence to the International Organization of Computer Evidence (IOCE), which has representation in most of the G-8 countries.

In May 2000, the NIPC attended a G-8 industry/law enforcement conference in Paris, France. This meeting, which included individuals representing industry and consumer groups, was structured to allow both industry and law enforcement officials to share ideas and concerns regarding the security of the Internet. Each participating country's contingent consisted of industry and government representatives, from a variety of agencies, and each country had one industry and one government representative make a presentation to the group about issues concerning their nation. Government officials were sensitized to the concerns of both industry and consumers, and industry and the public representatives were exposed to some of the challenges facing law enforcement and other government agencies in their struggle to provide a safe, secure environment for e-commerce. A subsequent meeting building on the success of the Paris forum is planned for October 2000.

The NIPC and International Investigations

Since the creation of the NIPC in February 1998, we have seen a significant increase in the number of investigations requiring international cooperation. The NIPC has provided an effective vehicle for coordinating these investigations. I will provide a few examples to demonstrate the issues raised by such investigations and how they have been addressed by the NIPC.

One example is the Solar Sunrise case, the code name for a multi-agency investigation of intrusions into more than 500 military, civilian government, and private sector computer systems in the United States during February and March 1998. These intrusions occurred just as the NIPC was being established. The intrusions took place during the build-up of United States military personnel in the Middle East in response to tensions with Iraq over United Nations weapons inspections. The intruders penetrated at least 200 unclassified U.S. military computer systems, including seven Air Force bases and four Navy installations, Department of Energy National Laboratories, NASA sites, and university sites. The timing of the intrusions, and the fact that some activity appeared to come from an ISP in the Middle East, led many U.S. military officials to suspect that this might be an instance of Iraqi information warfare. The NIPC coordinated an extensive interagency investigation involving FBI Field Offices, the Department of Defense, NASA, Defense Information Systems Agency, Air Force Office of Special Investigations, the Department of Justice, and the Intelligence Community. Internationally the

NIPC worked closely with the Israeli law enforcement authorities. Within several days, the investigation determined that two juveniles in Cloverdale, California, and individuals in Israel were the perpetrators. This case demonstrated the critical need for an interagency center to coordinate our investigative efforts to determine the source of such intrusions and the need for strong international cooperation. Israeli authorities are preparing to prosecute the chief defendant in their case in the summer of 2000.

More recent cases demonstrate how much international cooperation has improved in this area. In February 2000, the NIPC received reports that CNN, Yahoo, Amazon. Com, e-Bay, and other e-commerce sites had been subject to "Distributed Denial of Service" (DDOS) attacks. The NIPC had issued warnings in December 1999 about the possibility of such attacks, and even created and released a tool that victims could use to detect whether their system had been infiltrated by an attacker for use against other systems. When attacks did occur in February, companies cooperated with the NIPC and our National Infrastructure Protection and Computer Intrusion Squads in several FBI field offices (including Los Angeles and Atlanta) and provided critical logs and other information. Within days, the FBI and NIPC had traced some of the attacks to Canada, and subsequently worked with the Royal Canadian Mountain Police to identify the suspect. The Royal Canadian Mounted Police (RCMP) arrested a juvenile subject in April 2000, and charges are expected to be brought shortly for at least some of the attacks. The unprecedented speed and scope of this investigation was evidence of the great improvement made in our ability to conduct large scale, complex international investigations.

Another example involves the compromise between January and March 2000 of multiple e-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom by a hacker known as "Curador." Curador broke into the sites and apparently stole as many as 28,000 credit card numbers, with losses estimated to be at least $3.5 million. Thousands of credit card numbers and expiration dates were posted to various Internet websites. After an extensive investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (Wales, UK) Police Service in a search at the residence of "Curador," whose real name is Raphael Gray. Mr. Gray, age 18, was arrested in the UK along with a co-conspirator under the UK's Computer Misuse Act of 1990.

This case was predicated on the investigative work by the FBI, the Dyfed Powys Police Service in the United Kingdom, Internet security consultants, the RCMP, and the international banking and credit card industry. This case illustrates the benefits of law enforcement and private industry, around the world, working together in partnership on computer crime investigations.

Most recently, companies and individuals around the world by the "Love Bug," a virus (or, technically, a "worm") that traveled as an attachment to an e-mail message and propagated itself extremely rapidly through the address books of Microsoft Outlook users. Investigative work by the FBI's New York Field Office, with assistance from the NIPC, traced the source of the virus to the Phillippines within 24 hours. The FBI then worked, through the LEGAT in Manila, with the Phillippines' National Bureau of Investigation, to identify the perpetrator. The investigation in the Phillippines was hampered by the lack of a specific computer crime statute. Nevertheless, Onel de Guzman was charged on June 29, with fraud, theft, malicious mischief, and violation of the Devices Regulation Act. The speed with which the virus was traced back to its source is unprecedented. As a postscript, it is important to note that the Phillippines' government on June 14, 2000 approved the E-Commerce Act, which now specifically criminalizes computer hacking and virus propagation.

In addition to the matters mentioned above, we are currently working on numerous cases that require international cooperation. Because these are all pending matters, I cannot comment on them in this hearing. But I can say that the percentage of cases with an international element is increasing significantly.

These cases all illustrate the tremendous progress that has been made in the international arena. Countries around the world are addressing the cyber crime problem by creating new computer crime laws, establishing organizations and capabilities to handle investigations, and forging ties across international borders to facilitate investigations. While much work remains to be done, we can point with pride to the considerable advances that have been made in a very short time to strengthen international cooperation against cyber crime.

Conclusion

Cooperation among governments and between government and industry is the key to combating crime in cyberspace and making the Internet a safe and secure environment for e-commerce and communications. The NIPC has played an important role in fostering such cooperation. With the support of this committee and Congress as a whole, we hope to continue to build on this success.

Thank you.

Mr. HORN. Well, thank you very much. We appreciate that, Mr. Vatis.

Our next witness has traveled a long way to come here, so we are going to listen very carefully to the gentleman's testimony. It is Mr. Juris Reksna, chief of the State Police, Ministry of Internal Affairs in Latvia. He is accompanied by a translator, Tatjana Antonova. And we thank you very much for coming and sharing your information with us.

[NOTE.—The following testimony was delivered through an interpreter.]

Mr. REKSNA. Mr. Chairman and members of the subcommittee, I am honored here to represent the Republic of Latvia and I would like to express my gratitude for the invitation to participate in this hearing. The Latvian police and FBI cooperation has been extensive and has helped investigations in the U.S.A., resulting in the identification of violent criminals and the recovery of substantial amounts of funds for possible return to victims of crime in the U.S.A.

The cooperation increases every day, and the training that was provided by FBI and other U.S.A. law enforcement agencies has helped greatly. The funds, 500,000 U.S. dollars, provided by the U.S.A. Congress to Latvia for the purchase of equipment to fight organized crime, will allow Latvia to move into the cyber age more rapidly and to allow for the examination and analysis of data, and this will assist the U.S.A. in addressing crimes which have truly become transnational and the attempt to use Latvian banks on the Internet to escape detection.

The fight against cyber crimes is the responsibility of the criminal police of Latvia, which is a part of the National State Police. Three percent of our cases have international components. Most are threats that are being sent through anonymous Internet servers that are located outside the territory of Latvia, as well as attempts of hackers to break into financial institution computer systems.

As my time is limited, I will ask my interpreter to read the recent cases during the 2 years that took place in Latvia.

These are the synopses of criminal cases that have taken place: The so-called Terrorist Victor case. In March 1997, information was received about an explosive device placed in a shop. The police had neutralized this device. Shortly after that, e-mail threats have been sent by an anonymous person who called himself Victor, claiming to continue terrorist acts and demanding ransom.

As a result of investigation it was determined that Victor telephoned from a mobile phone that was illegally connected to the networks of Sweden, Norway and Finland. As a result of joint efforts made by law enforcement agencies from Sweden, Norway, Finland, Estonia, Austria, Russia, the U.S.A., Victor was identified. He was sentenced for 7 years in prison.

In the Lowes Home Improvement Center bombing case in North Carolina an individual planted several explosive devices in the stores which exploded and injured five persons. The criminal demanded money from the company and stated it should be wired to Paritate Bank in Latvia. The Latvian police, in coordination with the FBI LEGAT and the FBI office in Charlotte, NC, were able to track telephone calls, provide information on the account holder in the U.S.A. and his use of the bank's Internet banking service, which he thought would be difficult to trace because of the Internet and the location of the bank in Latvia.

The case of "stockgeneration.com" is worth mentioning as well. This pyramid scheme using the Internet was having money wired to Rietumu Bank in Latvia and attempted then to wire transfer it to accounts in Russia and elsewhere. The case is ongoing and being worked in conjunction with LEGAT Tallinn, the Boston division of the FBI, the Securities and Exchange Commission in Boston, and the Internal Revenue Service. Cooperation between the United States and Latvia and Estonia has resulted in the freezing of $5.5 million for potential return to U.S. victims.

Cyber crimes have really become transnational. Therefore, the following measures should be taken urgently to ensure our success in battling cyber crimes.

Joint international training in order to improve international response to cyber intrusions; close cooperation is necessary with all the partners on an international and national level in order to prevent and investigate cyber crimes more effectively; we should continue to develop and improve the current legislation in this issue; the Internet has become a major aspect of everyday life for the world's society. That is why international cooperation, mutual understanding and support is vitally important in order to improve our capabilities to locate and identify criminals.

Thank you for your attention.

[The prepared statement of Mr. Reknsa follows:]

Mr. Juris Reknsa

Chief of State Police
Ministry of Internal Affairs, Latvia

Before the

Committee on Government Reform

Subcommittee on Government Management, Information and Technology

"Computer Security: Cyber Attacks – War Without Borders"

July 26, 2000

Introduction

I am honored here today to represent the Republic of Latvia and to express my gratitude to the Congress of the United States of America for the invitation.

Having this opportunity, I would like to express the gratitude of the Government of the Republic of Latvia and of the State Police of the Republic of Latvia and me personally as its Chief, for the invaluable technical and other assistance provided by the United States in the battle against organized crime.

The United States of America was one of the first to recognized the independence of the Republic of Latvia by showing its understanding and support.

Since regaining independence (de jure) in 1991, Latvia pays special attention to the strengthening of democratic state institutions and Latvia, as in any other states, the opposition to the democratic process and the Rule of Law is considered to be part of the national security program.

The State Police of Latvia is state institution which has an obligation to defend a persons' life, health, rights and freedoms, property, the interests of society and the state from criminal and other unlawful offences.

The tasks of State Police of Latvia, according to Latvian Legislation, are the following:

- to guarantee the security of persons and society,
- to prevent criminal offences and other illegal offences,
- to detect criminal offences, to search for persons, who committed criminal offences,
- to render legal assistance to persons, institutions, undertakings and organizations in defending their rights and realization of their legal obligations,
- to enforce administrative and criminal penalties in the framework of its competence.

The main structural units of State Police are the Public Order Police and Criminal Police. The task of the Public Order Police is to guarantee public order, to fight against crime and to guard special objects. The functions of the Criminal Police are to prevent major crimes, to detect them and to search for persons, who hide from investigation and the court and avoid prosecution or are fugitives.

The fight against cyber crimes is the responsibility of the Criminal Police.

1. The proportion of transnational crimes, as a percentage of all crimes in Latvia is approximately 3%. Most are threats, that are being sent through anonymous Internet servers, that are located outside the territory of the Republic of Latvia as well as attempts of "hackers" to break into financial institution computer systems. In this area, the criminal cases are mostly detected thanks to the personal contacts of the computer specialists of Criminal Police of Latvia in cooperation with their colleagues abroad.

During the last five years, in the area of computer blackmail, the most noteworthy was the criminal case of an extorntionist "Victor". In March of 1997 one of the Varner Hakon Investment Corporation's shops in Riga received a message about the poisoning of their food products. Shortly thereafter, – on 19 March, the newspaper editorials received information about an expolosive device placed in a clothes shop named "Dressman" which belongs to the Latvian – Norwegian joint venture firm "Varner Baltics". "OMEGA", the special response unit of the Ministry of the Interior arrived in the shop and in one of the fitting rooms found a radio controlled explosive device, that was neutralized. From 20 May till 8 July, the management of the shop through Internet e-mail, received threats from an anonymous person, who called himself "Victor", claiming further possible terrorist acts in the shops belonging to this concern, unless this individual received 1,1 million USD. The extortionist phoned more than 30 times.. In May, the Ministry of the Interior established an operational detection group that was staffed by computer specialists. In the investigation of this crime, law enforcement agencies frm Sweden, Norway, Finland, Estonia, Austria, Russia and the United States of America, as well as Interpol and FBI cooperated. As a result of investigation it was determined that "Victor" telephoned from a mobile telephone that was illegally connected to the mobile telephone communications networks of Sweden, Norway and Finland, and that by using the Internet, from the neighboring state of Estonia, sent threatening letters via e-mail to the above mentioned concern.. As a result of these joint efforts ,"Victor" was identified. The offender was convicted and he was sentenced to 7 years of imprisonment in a maximum security prison.

Similarly, in the Lowe's Home Improvement Centre bombings case in North Carolina, an individual planted several explosive devices in the stores which exploded and injured five persons. He demanded money from the company and stated it should be wired to Paritate Bank in Riga, Latvia. The Latvian Organized Crime Bureau, in coordination with the FBI LEGAT and the FBI Office in Charlotte, North Carolina were able to track telephone calls, provide information on the account holder and his use of the bank's Internet banking services, which he thought would be difficult to trace because of the Internet and the location of the bank in Latvia. The Latvian Police, with the rapid assistance of the bank, were able to discover the true identity of the subject in the United States and to obtain his Internet Provider (IP) address, which was used to track him down and to provided information for a search warrant. The subject confessed and is awaiting sentencing.

As in the Maxim-Pi2000 case, subject(s) are stealing data base information from "e-commerce" companies, such as "CD Universe" and "Amazon.com" and demanding ransom or risk disclosure or sale of the information. Ransom in this case was to be wired to Hansabank in Riga, Latvia. The Economic Police assisted in obtaining banking information, which is being used to attempt to locate subject(s) and the iInvestigation is ongoing.

The case of "stockgeneration.com" is worth mentioning as well. This Pyramid scheme, using the Internet, was having money wired to Rietumu Bank in Latvia, and attempted to then wire transfer it to accounts in Russia and elsewhere. The case is ongoing and being worked in conjunction with LEGAT Tallinn, the Boston Division of the FBI, the Securities and Exchange Commission in Boston and the Internal Revenue Service. Cooperation between the United States and Latvia and Estonia has resulted in the freezing of 5,500,000 USD for potential return to US victims.

LEGAT Tallinn and the Latvian Police are also working on three other matters, all with similar methods and money movement through banks of Latvia, which offer Internet Banking services, which make the account holder anonymous, or at the very least hard to identify. It also changes the law enforcement theory that you should follow the money. The money movements on the Internet are so rapid and the Bank Privacy laws make the investigation of the crime more complex, requiring Mutual Legal Assistance Treaty (MLAT) requests. While these are faster then the former Letters Rogatory (Diplomatic Channel) process, it is still light years behind cyber and Internet banking.

Another ongoing criminal investigation, which has been active for seven months, was initiated based on the criminal activities of a Latvian firm "Logos Center". This agency, "Logos Center", was initially engaged in producing video movies of pornographic character and their legal distribution, including the implementation of foreign orders. However, investigation by the Computer Crimes Center, and the Criminal Police, determined that this was a front for the involvement of minors in prostitution and the production pornographic movies with minors. Firm "Logos Center" created Internet site, where it advertised its photo models, entered photos of sexual intercourse and as well as offered "escort services" for its users abroad. Moreover the users of the "Logos Center" site could enter into sites of other firms, where there were popularized zoophylia and child pornography. One of the charges pending against these offenders is the distribution of child pornography on the Internet.

As my time is limited, I will not be able to tell you about all the examples of our successful cooperation. There is no lack of such examples.

2. During the investigation of "Victor", the Criminal Police of Latvia many times applied for assistance to FBI and the FBI responded to our request.

In connection with the investigation of the above mentioned criminal case on child pornography on the Internet, officers of the Criminal Police of Latvia through the National Bureau of Interpol, have requested the FBI to identify IP addresses of WEB – servers located in the USA and to identify by the e-mail addresses, the foreign clients of the firm "Logos Center". We hope to receive this informnation in the near future.

3. The Latvian Police and FBI cooperation has been extensive and has helped investigations in the US, resulting in the identification of violent criminals, and the recovery of substantial amounts of funds for possible return to victims of crimes in the US. The cooperation increases every day and training and technical assistance provided by the FBI and other US law enforcement agencies has helped greatly. The funds (500 000 USD) provided by the US Congress, for the purchase of equipment to fight organized crime, will allow Latvia to move into the cyber age more rapidly and to allow for the examination and analysis of data and this will assist the US in addressing crimes, which have truly become transnational, and attempt to use Latvian banks and the Internet to escape detection.

4. We consider that the necessary priorities for investigation of cyber crimes are agreements between law enforcement agencies and ISP (Internet Service Provider) of different states, on data storage for a period of not less than three months. In all the cases of international cyber crimes, the officers of the law enforcement agencies had to address ISP administrators who control the data exchange using WEB – servers. If the control data is not stored for more than one month, as a practical matter, it is not possible to detect concrete IP addresses, from which the information was sent (threats, using e – mail; spreading of computer viruses, attempts of intrusion into the computer systems, spreading of child pornography, etc.)

5. In order to the improve fight against cyber crime on a national and international level, we would recommend that there be organized additional practical training on the use of modern software; investigative and security software; e-mail to be traced to it's source; remote PC and Network monitoring; tracking and the location of stolen electronic documents; and the detection of intrusion threats into computer data bases.

6. Officers of the Criminal Police of Latvia cooperate with representatives of the private sector, for example, in cyber crime prevention and detection with specialists of computer services of the largest Latvian commercial banks. The computer specialists of commercial institutions many times furnish information to Criminal Police on attempts of intrusion into the data bases of banks and commercial institutions and often have carried out mutual activities with computer specialists from Police. Here I would again mention the cooperation in identifying the criminal who committed the bombings in the North Carolina stores in the USA.

7. The legislation in the field of information technologies in Latvia consists of:

- Law On State Secrecy (1996.17.10),
- Law On Information Publicity (1998.29.10),
- Law On Person Data Protection (2000.23.03.)
- Regulations of the Cabinet of Ministers of the Republic of Latvia Nr. 225 "State secrecy protection regulations" (1997.25.06.)
- Regulations of the Cabinet of Ministers of the Republic of Latvia Nr. 106 "Information system security regulations" (2000.21.03.)

In Latvia it is possible to hold someone criminally liable under the following provisions of Criminal Law (Articles 241 – 245) – for unauthorized access to computer systems, unauthorized acquisition of computer software, spreading of a computer virus, violation of safety provisions regarding information systems – regardless of it being committed under avaricious, revenge or other motives (ideological, political as well as for purpose of demonstrating ones superiority in the knowledge of computer technologies).

8. In order to improve the procedure of obtaining evidences on an international level, in the near future, every interested state needs to develop the procedures and regulations for computer seizures, operative investigations and examinations, aiming for uniform legislation of legal procedures. This is necessary because of the international character of cyber crime, and because criminals using the Internet in one state, can commit a crime that violates not only persons and laws of one state, but also attacks state infrastuctures (financial, defence, power industry, transport, etc.). In such cases, it will be necessary to simplfy the procedure for law enforcement officers, to obtain material evidences, under appropriate legal procedure (data carrier seized from criminals in other state, including data base copies, correspondance documents, etc.), for use in their investigations.

9 – 10. Every state has to establish an organization with responsibility for the following tasks:

- coordination of operative international cooperation, by means of well considered communication and contact through a system of specially designated persons or liaison officers,
- Monitoring of computer networks (mainly in Internet global net) in order to fight high – tech crime;
- The establishment of working contacts with Internet providers,
- In the frameworks of FBI/ NIPC cooperation, to provide an exchange of information on the trends of cyber crime investigations,
- to organize common training for employees.

A special division (computer specialists and opertive officers) of Criminal Police of Latvia has been established, in order to find and identify cyber criminals, as well as to inspect and examine computer equipment. This structural unit in perspective will be responsible for storage of critical international and other information that is to be used operationally. The above mentioned unit also participates in the detection of cyber crimes.

Crimes which involve computers and the Internet have become a reality of social life. Therefore operative international cooperation, mutual understanding and support in the fight against this kind of crime is necessary.

Thank you for the attention.

Mr. HORN. That is perfect timing if I ever saw it. We just have a vote now, so we are going to have to recess for about 15 minutes here and vote and come back. Two votes, so it might be 20 minutes. So we are in recess.

Mr. DAVIS. Mr. Chairman, could I ask unanimous consent that my statement be put in the record?

Mr. HORN. Without objection, the gentleman's opening statement will be put after the ranking member as if read. Thank you. With that, we are in recess for 20 minutes.

[Recess.]

Mr. HORN. The recess is over and we will go to the next witness, Mr. Stefan Kronqvist, chief, Computer Crime Unit, National Crime Investigation Department, Sweden. We thank you for coming the long flight you did have. So please proceed, and if you could summarize it in 5 to 7, 8 minutes, that would be appreciated.

Mr. KRONQVIST. Thank you, Mr. Chairman, Congressman Turner. Thank you for the opportunity to appear before you today to describe the situation on combating cyber crime from the Swedish point of view.

On the reorganization of the Swedish police force, the National Criminal Investigation Department is the central responsible authority for operational police activities. Responsibilities of the national CID include criminal intelligence service, certain qualified criminal investigations and support to the local police authorities. The NCID is functioning as central level coordinator for the combat against organized crime.

Further, the NCID is responsible for operational international police cooperation, operation and serving as National Central Bureau of the Interpol and the national Europol units.

The Information Technology Crime Unit of the NCID has instructions to maintain and develop national support activities in order to assist the local police authorities in surveying and investigating IT crime. The unit provides training, developmental tools and techniques and also carries out operational activities by conducting house searches and interviews and analyzing seizures and also by tracing and identifying persons who use the Internet and its services and functions as targets or means in the commission of crime.

Recently, we established a 24-hour service, one reason being that Sweden had joined the G–8 Network contact point for high-tech cases.

The IT unit at NCID is processing some 500 cases yearly. Of these cases about 50 percent are Internet related. Practically all Internet cases have an international component. The Internet knows no boundaries and no border lines.

For a good many years the NCID has enjoyed a state of close and comprehensive cooperation with the FBI. We have had several investigations where we worked with the FBI and perhaps the best known case would be the E911 case in which our unit cooperated with the FBI in an effort to trace and identify a Swedish suspect who, by means of illegal telecommunication, periodically locked the E911 lines in a major area in Florida.

One element of this cooperation was to set up a tracing team with Swedish and U.S. telecommunication operators. This was a rather complex operation, which could not have succeeded without the professional skill and dedication of the units and the investigators involved.

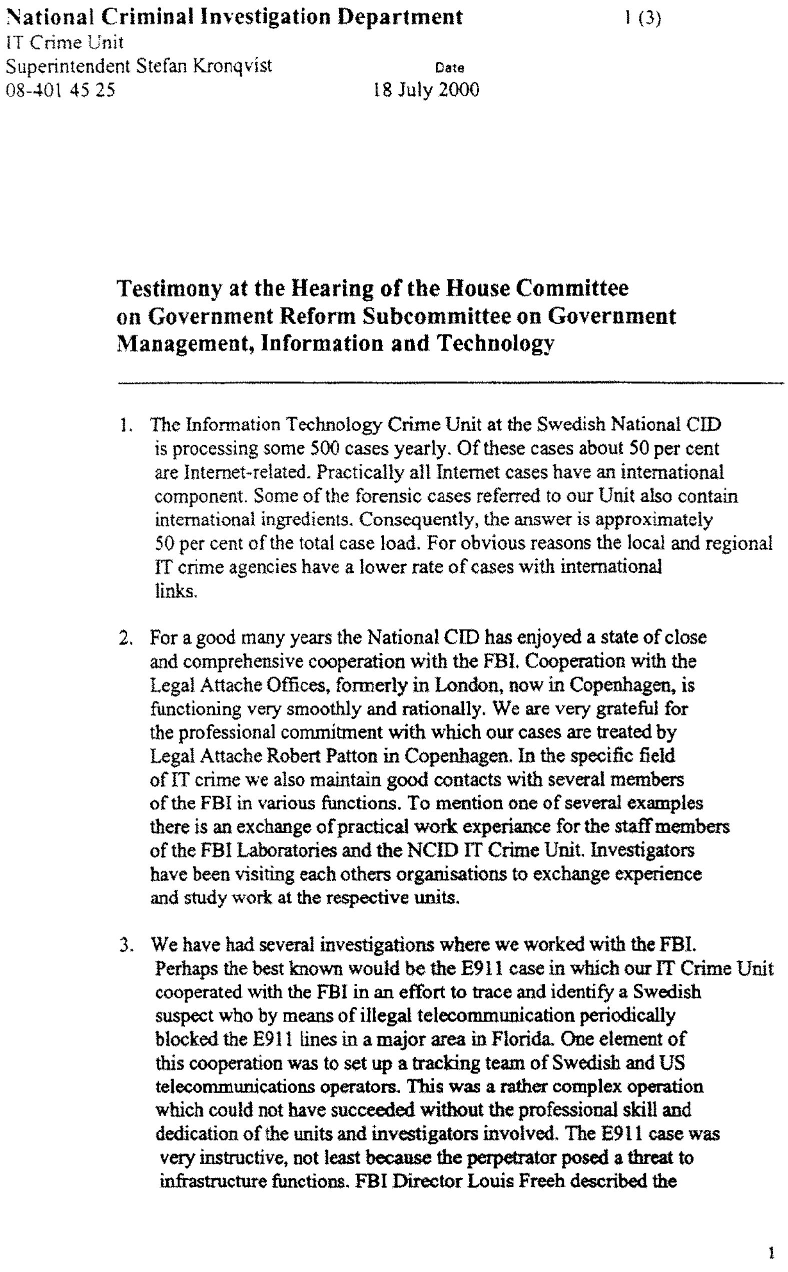
The E911 case was very instructive, not least because the perpetrator posed a threat to infrastructure functions. FBI Director Mr. Louis Freeh described the incident "as a dress rehearsal for a national disaster."

The main problem we are facing in Internet crime is obtaining access to useful information from foreign Internet providers and responsible Web managers. Normally, a provider asks for a court order, subpoena, or other form of domestic disposition before information is supplied. Such a decision must be preceded by an international letter rogatory, a time consuming procedure, as we all know. It is my understanding that certain criminal operators are well aware of this.

One way of addressing this problem that suggests itself would be international agreements to release subscriber information and logged IP addresses and other useful information to law enforcement authorities in another country without the requisite of a formal rogatory request. The transmission of information would be handled via special contact points in order to secure authority and make sure that the information does not fall into the wrong hands.

In order to ensure the quality of documents or information, probably some kind of authorization or licensing of Internet operators might be a possible alternative. You may probably not get to the actual criminals that way, but what do they care about regulations anyway? Thank you for your attention.

[The prepared statement of Mr. Kronqvist follows:]



National Criminal Investigation Department 1 (3)
IT Crime Unit
Superintendent Stefan Kronqvist Date
08-401 45 25 18 July 2000

Testimony at the Hearing of the House Committee on Government Reform Subcommittee on Government Management, Information and Technology

1. The Information Technology Crime Unit at the Swedish National CID is processing some 500 cases yearly. Of these cases about 50 per cent are Internet-related. Practically all Internet cases have an international component. Some of the forensic cases referred to our Unit also contain international ingredients. Consequently, the answer is approximately 50 per cent of the total case load. For obvious reasons the local and regional IT crime agencies have a lower rate of cases with international links.

2. For a good many years the National CID has enjoyed a state of close and comprehensive cooperation with the FBI. Cooperation with the Legal Attache Offices, formerly in London, now in Copenhagen, is functioning very smoothly and rationally. We are very grateful for the professional commitment with which our cases are treated by Legal Attache Robert Patton in Copenhagen. In the specific field of IT crime we also maintain good contacts with several members of the FBI in various functions. To mention one of several examples there is an exchange of practical work experiance for the staff members of the FBI Laboratories and the NCID IT Crime Unit. Investigators have been visiting each others organisations to exchange experience and study work at the respective units.

3. We have had several investigations where we worked with the FBI. Perhaps the best known would be the E911 case in which our IT Crime Unit cooperated with the FBI in an effort to trace and identify a Swedish suspect who by means of illegal telecommunication periodically blocked the E911 lines in a major area in Florida. One element of this cooperation was to set up a tracking team of Swedish and US telecommunications operators. This was a rather complex operation which could not have succeeded without the professional skill and dedication of the units and investigators involved. The E911 case was very instructive, not least because the perpetrator posed a threat to infrastructure functions. FBI Director Louis Freeh described the

incident as "a dress rehersal for a national disaster".

4. The most important thing would be to have IP addresses logged and make sure that they are stored and kept in a readable and searchable condition. As to Internet Service Providers it is important that the information is technically quality-proof, for instance that system clocks, etc., are correct. Sometimes the question arises whether or not to keep a system open in order to be able to trace an ongoing intrusion. My advice in these cases is always to weigh up the pros and cons in terms of potential damage and investigative interests.

5. At the present time a series of three-week methodology-orientated courses are being arranged over a period of two years for a total of 120 IT crime investigators, a number of prosecutors included. The course is an extention of a three-month basic technical training course given last year. Available at international level since 1993 are training courses for European IT crime investigators organized by the ICPO-Interpol. There has been a proposal to provide international training in cyber intrusion detection. Besides methodology and technical subjects, such a training course could also contain instructive information about international regulations and contact channels.

6. In our opinion there is a differences of attitude towards a working relationship on the part of the private sector, often depending on the gravity of the crime. In cases where great values have been lost or are in danger of being lost the private sector is often prepared to cooperate. The willingness of companies to report crimes or assist investigations involving a third party is also dependent on whether they fear they may invite criticism of their own internal IT security. The Swedish National Crime Prevention Board recently publicized a poll on IT crime in medium-sized businesses and organizations which confirms this situation.

7. The specific act of cyber intrusion is long since a criminal offence under Swedish law. What is now being discussed are the legal coercive means of detecting, monitoring and tapping telecommunicaitons to and from suspect criminals. These matters are currently being reviewed by the Swedish Ministry of Justice. The purpose is to adapt regulations to modern computer and telecommunication technology.

8. The major problem we are facing in coping with Internet crime is that of obtaining access to useful information from foreign Internet Service Providers and responsible Web managers. Normally, the provider asks for a court order, subpoena or other formal domestic disposition before information is supplied. Such a decision must be preceded by an international letter rogatory, a time-consuming procedure as we all know. It is my understanding that certain criminal operators are well aware of this. One way of addressing these problem that suggests itself would be international agreements to release subscriber information and logged IP addresses to the law enforcement

authorities in another country without the requisite of a formal letter rogatory request. The transmission of information would be handled via special contact points in order to secure authority and make sure that the information does not fall into the wrong hands.

9. Regulations requiring anyone conducting business or organizational or related activities on Internet to possess the ability and knowledge to provide adequate information to law enforcement agencies to assist criminal investigations. Some kind of authorization or licencing of Internet operators might be a possible alternative. You may probably not get to the actual criminals that way but what do they care about regulations anyway?

10. The Swedish Government is presently in the process of setting up a national Computer Emergency and Critical Incident Response Function. At the present moment opinions vary as to how such a function should be organized and operated. The Swedish police hold the view that such an agency should be managed by the police or at least contain a manifest law enforcement element. An organization without police participation would be without the powerful information and contact channels accessible to the police. Also, there is the risk of not being able to protect important third party interests. It has further been argued that such a function should not be permitted to access information from the private sector if businesses face the risk of ending up in an undesired criminal investigation because a crime was reported to the police. It will therefore be extremely interesting to take note of the experiences of the NIPC.

National Criminal Investigation Department 1 (1)
IT Crime Unit
Superintendent Stefan Kronqvist Date
08-401 45 25 18 July 2000

Short description of the National CID and the IT Crime Unit

Under the organization of the Swedish police force the National Criminal Investigation Department is the central responsible authority for operational police activities with the exception of those subordinate to the Swedish Security Service and the Economic Crimes Bureau. The responsibilities of the National CID include criminal intelligence service, certain qualified criminal investigations and support to the local police authorities. The National CID is functioning as central level coordinator of the combat against organized crime.Further, the National CID is responsible for operational international police cooperation and serving as National Central Bureau of the ICPO-Interpol and National Europol Unit.

The IT Crime Unit of the National CID has instructions to maintain and develop national support activities in order to assist the local police authorities in surveilling and investigating IT crime. The unit provides training, methodology and technology development and also carries out operational activities by conducting house searches and interviews and analysing seizures and, also, by tracing and identifying persons who use Internet and its services and functions as targets or means in the commission of crime. The unit serves as contact point for international police cooperation in this specific subject field. A year ago the IT Crime Unit introduced a 24-hour service, one reason being that Sweden had joined the G8 Network of 24-Hour Contacts for High-Tech cases.

National Criminal Investigation Department 1 (1)
IT Crime Unit
Superintendent Stefan Kronqvist
08-401 45 25

Date
18 July 2000

Brief summary of Swedish legislation on Computer Crime

Most IT-related crimes are provided for under traditional penal law. However, there are special provisions for computer intrusion (breach of daa secrecy) Penal Code, Chapter 4, Section 9c, computer fraud (PC, Chapter 9, Section 1) and the Copyright Act on computer programmes and the legislation on liabilities referring to electronic bulletin boards. The recently updated legislation on personal integrity (Personal Data Act) is highly apdated to the modern IT society.

The legislation on Criminal Porcedures is being revised for adaption to modern technology. The same is the case with the special legal provisions on the confiscation of property and assets. For instance data cannot be independently seized and forfeited, this procedure can presently be applied only to material objects.

Mr. HORN. Well, we thank you very much. That is a very fine presentation, and we can learn a lot from it.

Our next witness is Mr. Juergen Maurer, detective chief, superintendent, German Federal Police Office.

Mr. MAURER. Mr. Chairman, ladies and gentlemen, I am very pleased and sincerely honored to receive the opportunity to address the members of this honorable committee.

My name is Juergen Maurer. I am a Leitender Kriminaldirecktor of the German Criminal Police Office, or BKA. I am the head of the Subdivision Central Services within the BKA and, among others, responsible for the undercover program and the foreign liaison program of the BKA. In this context, allow me to give you some short background information about our office.

The BKA was founded in 1951. In Germany, based on our Constitution, police work is in general within the jurisdiction of the Federal states. The BKA law constitutes an exemption from this principle. As a result of this exemption, the BKA is, among others, the German National Center Bureau of Interpol and the main law enforcement agency in the field of international organized crime and terrorism cases. The BKA is also the primary police agency dealing with cyber crime.

The bulk of cyber crime cases handled by the BKA has an international component. A special reporting system has been set up for information and technology crime and shows that about 50 percent of ICT cases have an international component.

Cooperation with partner agencies from abroad is mainly through the 24-hour contact points for international high-tech and computer-related crime established by the G–8 countries. In addition, there are contacts with the United States using our BKA liaison officers at our Embassy in Washington, DC, or the FBI liaison officer posted to Frankfurt, Germany, on a case-by-case basis. Contact with the NIPC on a case-to-case basis has occurred so far only in connection with the distributed denial of service attacks in February this year.

The case showed that even though the cooperation was very good, there is still a need to establish a more efficient and effective way of exchanging information. In late June this year, representatives of the BKA and NIPC discussed possibilities to enhance the cooperation.

The overall investigative cooperation of BKA and FBI has a long tradition and has proved very successful. We work together in a significant number of organized crime and white collar crime cases. There has also been a very successful cooperation with the FBI concerning fugitive cases.

Within the BKA, the IT crime section has about 30 officers and the following tasks: collection and analysis of IT crime information; national reference point on IT crime; assistance and training for other investigative units; analysis of data carriers and storages; Internet investigation; and the so-called data network patrol.

In this unit, 15 police officers in an overt, nonconcealed manner are surfing the net and developing criminal cases in identifying the perpetrators. In 1999, around 1,100 cases with the suspicion of crime were detected; 90 percent of these cases were child pornography cases, 81 percent of these cases had an international component; 62 percent of these cases had a connection with the United States.

What should have priority in the future? First, victims of cyber intrusions as well as ISPs should keep and make available log files providing information about the IP addresses used by the criminal or other information that may help identify the criminal.

It would also assist investigators if the ISP created technical prerequisites for the surveillance of on-line communications comparable to telecommunications interception for them to be conducted straight away if required by law.

Second, there is already a variety of training and advanced training courses organized on the international level. However, more training should be provided. There is a need to create uniform training standards for investigators at the international level and establish points of contact for partner agencies from abroad to guarantee a great information flow.

Third, many victimized companies in Germany are still hesitant to file a criminal complaint with the law enforcement agencies because they feel loss of prestige. For the benefit of law enforcement, it seems important to forge cooperation partnerships with the system administrators of the victims to obtain the required information more quickly. In urgent cases; for example, extortion and danger to life and limb, access to the raw data should be possible without having to go through the time consuming standard formalities under international law.

Also some types of computer crime and cyber intrusions in particular require an immediate response by the law enforcement community since data needed as evidence are usually stored for a short period of time only.

That was pretty much I wanted to stress. Thank you very much for your attention.

[The prepared statement of Mr. Maurer follows:]

Mr. Juergen Maurer

Detective Chief Superintendent
German Federal Police Office

Before the

Committee on Government Reform

Subcommittee on Government Management, Information and Technology

"Computer Security: Cyber Attacks – War Without Borders"

July 26, 2000

Ladies and Gentlemen,

I am very pleased an sincerely honored to receive the opportunity to address the members of this honorable committee.
My name is Jürgen Maurer, I am a Leitender Kriminaldirektor of the German Federal Criminal Police Office, or Bundeskriminalamt.
After high school and military service I finished my college and university education with academic degrees in economics and social sciences.In July 1981 I started working with the German Federal Criminal Police. Aside my work in the field of white collar and organized crime I was sent as the senior police liaison officer to our German Embassy in Washington DC and served there from September 1997 untill March 2000.
Since then, I am the head of the *Subdivsion Central Services* within the German Federal Criminal Police Office and among others responsible for the under cover program and the foreign liaison program of the Bundeskriminalamt.

In this context let me allow to give you some short back ground information about our office:
The Federal Criminal Police Office, BKA or Bundeskriminalamt was founded in 1951. The work of the BKA is based on the BKA-law in the version of 1997. In Germany , based on our constitution, police work is in general within the jurisdiction of the federal states. The BKA-law constitutes an excemption from this principle.

As a result, the BKA is

- the central police agency for the exchange of information,
- the German national central bureau of Interpol,
- the first agency in the field of international drug cases and smuggling of weapons, counterfeiting of currency and other serious cases of international organized crime and terrorism,
- the responsible office for the physical protection of the members of the German government and of foreign dignitaries.

The BKA has its headquarters in Wiesbaden, Hessia, and regional offices in Bonn and Berlin. As of the end of 1998, around 4,800 people were working for the BKA. In that number are included the 1,500 BKA-police-officers. The BKA is the strongest investigative agency in Germany and has sent around 60 police liaision officers abroad.

Our answers concerning the questions of the House Subcommittee on Government Management, Information and Technology are as follows:

1. ***Can you estimate what percentage of your cases have an international component?***

   Since the BKA is responsible for processing international communications in its capacity as National Central Bureau of I.C.P.O-Interpol and as the central c.i.d. agency in Germany, the bulk of cases handled by the BKA has an international component. A special reporting system has been set up for ICT Crime (Information and Technology Crime) wich includes strictly German cases as well as cases with an international component. The percentage of ICT cases with an international component is estimated at about 50 per cent.

2. ***How would you rate your cooperation with the Federal Bureau of Investigation (FBI)/National Infrastructure Protection Center (NIPC) on cyber intrusion cases?***

   Co-opertion with partner agencies from abroad is mainly through the 24-Hour Contact Points for International High-tech and Computer-related Crime established by the G8 countries. In addition, there are contacts with the United states using our BKA liaison officers at our embassy in Washington, DC, or the FBI liaison officer posted to Frankfurt/Germany on a case-to-case basis.

   Contact with the National Infrastructure Protection Center (NIPC) on a case-to-case basis has occurred only once. In connection with the "distributed denial of service attacks" in February this year, a request for information was forwarded to the NIPC via the German liaison officer in Washington, DC. However, co-operation proved

highly problematic. The case showed, that there is the urgent need to establish a more efficient and effective way of exchanging information.
In late June this year representatives of the BKA and NIPC discussed possibilities to enhance the cooperation.
Also in 1999, a BKA officer attended the International Computer Crime Conference hosted by NIPC.

3. ***Could you comment on any past investigations which you worked with the FBI/NIPC?***

There have been no past investigations in which we worked with the NIPC. However, the investigative co-operation of BKA and FBI has a long tradition and has proved very succesful. We worked together in a significant number of organized crime and white collar crime cases. There has also been a very succesful cooperation with the FBI concerning fugitive cases.

4. ***What measures would be useful to you as investigators regarding record keeping by Internet Service Providers or by victims of cyber intrusions?***

Victims of cyber intrusions as well as Internet Service Providers (ISP) should keep and make available log files providing information about the IP adresses used by the criminal or other information that may help identify the criminal.
It would also assist investigtors if the ISP created technical perequisites for the surveillance of online communications (comparable to telecommunications interception) for them to be conducted straightaway if required by law.
The data available should be forwarded to the requesting law enforcement agency without having to overcome major bureaucratic obstacles.

5. ***Regarding training, what training can be done on a national or international basis to improve international response to cyber intrusions?***

There is already a variety of training and advanced training courses organised on international level. For instance, Interpol's European Working Party on IT-Crime organises two training sessions per year which meet with a good response on the part of the participating countries. Unfortunately, the number of training sessions has to be limited to two per year for two reasons: there are only few police experts available to run such courses, and limited funds which do not permit to draw on external resources. However, more training of this type could be provided on an international level if more countries would be prepared to participate in this initiative in an active manner.

6. ***Can you please discuss your working relationship with the private sector in your nation in cases where they are the victims of or unwitting participants in a cyber intrusion?***

   Many victimised companies in Germany are hesitant to file a criminal complaint with law enforcement agencies because they fear a loss of prestige. However, if they opt to make a complaint, most of them are found to be co-operative. For the benefit of law enforcement it is important to forge co-operation partnerships with the system administrators of the victims to obtain the required information more quickly.

7. ***Can you discuss current or proposed legislation in your nation for addressing cyber instrusions?***

   Cyber Intrusions constitute a criminal offence pursuant to sections 202a – data spying -, 303a – alteration of data – and 303b - computer sabotage – of the German Penal Code. The Council of Europe is currently discussing uniform legislation for addressing this phenomenon.

8. ***What means can you suggest for improving the process of obtaining evidence internationally – protected seizures, transborder search and seizure, computer forensics, etc. ...?***

   We would like to suggest the following means for improvement: create uniform training standards for investigators at international level and – many countries have done this already – establish points of contact for partner agencies from abroad to guarantee a quick information flow. In urgent cases (extortion and danger to live and limb), access to the required data should be possible without having to go through the time-consuming standard formalities under international law.

9. ***What can you suggest to improve our capabilities to locate and identify criminals, and specifically the preservation of critical transactional data and other information that must be shared quickly?***

Some types of computer crime, and cyber intrusions in particular, require an immediate response by the law enforcement community, since data needed in evidence are usually stored for a short period of time only. Reverting to traditional means of legal assistance would cause long-term delays. Preservation orders may assist in the timely preservation of critical data relating to intruders who have made their way into a victims computer via several other computers by ensuring that the data at the previous point of entry are not deleted. However, data disclosure/transfer is not covered by the preservation order, which means that often necessary follow-up enquiries with other ISP are delayed or even prevented altogether as a result of lengthy legal assistance procedures.

10. ***Based on your own national experience, what can you suggest to other nations regarding governmantal organization to detect, warn of, and respond to cyber intrusions?***

There is a need to set up special communication channels which should be open 24 hours a day to process urgent and critical cases. In addition, there should be a central agency empowerd to take immediate action which is crucial to the entire investigation.

Mr. HORN. Thank you very much.

We will go out of order because we are trying to help on a situation that a member of the executive branch has here. So if you might, we are going to start with his testimony, since he has to be elsewhere.

John T. Spotila is the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget, which is part of the President's Executive Office of the President.

STATEMENT OF JOHN T. SPOTILA, ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS, OFFICE OF MANAGEMENT AND BUDGET

Mr. SPOTILA. Good morning, Mr. Chairman. Thank you for inviting me here to discuss administration efforts in the areas of computer security and critical infrastructure protection.

The President has given high priority to cyber security and the protection of our Nation's critical information assets. He understands the growing risks that our Nation faces from cyber threats and has taken a series of steps outlined in my written testimony to develop our cyber defenses. In his fiscal year 2000 budget, the President proposed some $2 billion for agency critical infrastructure protection and computer security programs. This would be an increase over last year's enacted total of $1.8 billion.

It would include funding to detect computer attacks, coordinate research on security technology, hire and train more security experts, and create an internal expert review team for nondefense agencies.

These initiatives are vitally important. Regrettably, many of our requests for security funds face an uncertain future in the appropriations process. We critically need funding for the National Institute for Standards in Technology and the Critical Infrastructure Assurance Office at Commerce, for the Federal computer incident response capability, and the Federal intrusion detection network at GSA, for public key infrastructure work at Treasury, and for the scholarship for service effort at the Office of Personnel Management and the National Science Foundation.

It has been particularly difficult to gain support for crosscutting initiatives, despite their importance to our computer security efforts. We should be more open to innovative approaches in this area and look for opportunity for synergy and interagency cooperation.

OMB plays a key role in government computer security efforts. In February, we issued important guidance to the agencies on incorporating security and privacy requirements in each of their fiscal year 2002 information technology budget submissions.

In the future, when requesting approval for information technology funds, agencies must demonstrate how they have built adequate security and privacy controls into the life cycle maintenance and technical architectures of each of their systems. Without an adequate showing, the systems will not be funded.

OMB Circular A–130 sets forth governmentwide policies for a wide variety of information and information resource management issues. It addresses agency management of information and information systems, including capital planning and investment control.

Appendix 1 sets privacy policy. The soon to be issued appendix 2 defines policy for information architectures and implementation of the Government Paperwork Elimination Act. Appendix 3 sets security policy.

Importantly, appendix 3 requires Federal agencies to adopt a minimum set of risk-based management controls. Four controls are described: assigning responsibility for security, security planning, periodic review of security controls, and management authorization.

These controls are intentionally not technology dependent. Instead, they focus on the management controls agencies need to assure adequate security. Technical and operational controls should support these management controls.

We believe, as GAO has said, that our computer security policies are properly focused on a risk-based cost-effective approach and reflect the right balance between strong security and mission needs. Good design and good planning are the keys to successful security. For good design, security must be compatible with and enable, not unnecessarily impede, system performance, business operations, and the mission.

When security unnecessarily slows the system or hinders the mission, users often work around it or ignore it completely. To work effectively, security must be part of the system architecture, built in so that users will buy in.

Good planning requires that we fund security and privacy as part of the life cycle costs for each system. To identify a true system cost and adequately plan for future system or program operations, we must account for all of the resources necessary to operate the systems, including security.

Our approach provides maximum flexibility for agencies so that they can make appropriate informed choices in applying necessary security controls that are consistent with their unique circumstances.

Most security problems come not from a lack of policy, but rather from ineffective or incomplete implementation of existing policies and guidance. We are very much aware of this risk in the Federal context. There is much more to be done before we reach full implementation of our existing security guidance.

As my written testimony describes, we are working on a number of specific projects to assist the agencies and enhance governmentwide security. These include testing a systematic process of identifying, assessing, and sharing effective security practices; finalizing security performance measures against which agencies can assess their security programs; creating a formal process for coordinating our governmentwide response to cyber incidents of national significance; and promoting more timely agency installation of patches for known vulnerabilities.

These are innovative efforts that show great promise. They need congressional support if we are to fulfill that promise. We appreciate your interest in all of these matters and look forward to continuing our close cooperation with the committee in this important area. We value our partnership with you and hope that this hearing will mark a further strengthening of our joint efforts on behalf of the American people.

Thank you.

[The prepared statement of Mr. Spotilla follows:]

STATEMENT OF THE HONORABLE JOHN T. SPOTILA
ADMINISTRATOR
OFFICE OF INFORMATION AND REGULATORY AFFAIRS
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
July 26, 2000

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me here to discuss Administration efforts in the areas of computer security and associated critical infrastructure protection. We know that our government and our nation rely increasingly on computer systems to support nearly every critical governmental and business function. Government and industry are now more interconnected than ever, operating in a shared risk environment, with our interdependence growing daily. The integrity and availability of our systems and, where appropriate, the confidentiality and privacy of information in those systems are today more important than ever.

Administration Actions

The President has given high priority to cyber security and the protection of our nation's critical information assets. He understands the growing risks that our nation faces from cyber threats. In May 1998, after reviewing the report of his Commission on Critical Infrastructure Protection, he issued Presidential Decision Directive 63, on "Critical Infrastructure Protection."

This Directive provided a framework for government action. It pointed out that interconnected computer systems are necessary for the provision of essential national services. It recognized that a potential future attack against the United States might take the form of a cyber attack against our critical computer systems. It acknowledged that government and industry face essentially the same risk in this area and must work in close partnership to mitigate that risk. Indeed, as today's hearing also recognizes, it took into account that this risk is shared globally.

The Directive also called on all Executive branch agencies to assess the vulnerabilities to their systems and the nation's critical infrastructures -- communications, energy, banking and finance, transportation, emergency services, and public health. It placed special emphasis on protection of the government's own critical assets and establishing the government as a model for information security. This is where OMB's primary role lies and where we have been concentrating our efforts.

To implement the Directive, the President appointed Richard Clarke of the National Security Council as the nation's first National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. Later, the National Security Advisor announced the appointment of Jeffrey Hunker as Senior Director for Critical Infrastructure Protection, in the Office of Transnational Threats. Both have worked tirelessly to increase national awareness of the scope of the problems in this area, working closely with OMB to help formulate sound approaches to addressing these problems.

The Directive called for the development of a detailed National Plan for Information Systems protection, so that we could better defend against cyber disruptions. It also established a Critical Infrastructure Assurance Office (CIAO) at the Department of Commerce to coordinate government interaction with industry, develop the national plan, and assist federal agencies in identifying and prioritizing their own critical assets.

The Directive also established at the FBI the National Infrastructure Protection Center (NIPC) as a national focal point for gathering information on threats to the nation's critical infrastructures. The NIPC's Director, Michael Vatis is also testifying before you today.

In January of this year, the President announced the issuance of version one of the National Plan for Information Systems Protection. He pointed out that the Plan was the first major element of a more comprehensive effort and that it would evolve and be updated as we increase our knowledge of our vulnerabilities and of emerging threats. The plan called for a number of government-wide and agency-specific security initiatives, as well as increased cooperation with industry and others in the private sector. In this last regard, we note that CIAO under the leadership of its Director, John Tritak, has worked with industry to build the Partnership for Critical Infrastructure Security, now comprising more than 130 representatives from major U.S. corporations. The Partnership is meeting this week in San Francisco.

In February of this year, in the wake of a series of distributed denial of service attacks against a number of major electronic commerce websites, the President held a Cyber Security Summit with key information technology leaders. At this summit, which I attended, the private sector leaders emphasized their desire to participate in partnerships with the government and with one another to facilitate the sharing of information on cyber attacks and common vulnerabilities.

The President's Chief of Staff, John Podesta, has been personally engaged in these security issues. He has directed the agencies to take specific actions to improve security and to report to him on the status of the security posture of their websites. Just last week, he delivered a major speech outlining the Administration's position on cyber crime legislative reforms designed to upgrade 21st Century law enforcement capabilities and also enhance privacy and civil liberties in cyber space.

The President's FY 2001 budget proposed approximately $2.0 billion for agency critical infrastructure protection and computer security programs out of a total information technology budget of about $40 billion. This security total is a 15% increase over the FY 2000 enacted total of $1.8 billion. It includes funding to help detect computer attacks, coordinate research on security technology, hire and train more security experts, and create an internal expert review team for non-defense agencies. These initiatives are vitally important.

Regrettably, many of our requests for security funds face an uncertain future in the appropriations process. It has been particularly difficult to gain support for cross-cutting initiatives, despite their importance to our computer security efforts. We should be more open to innovative approaches in this area and look for opportunities for synergy and interagency cooperation.

Several important cross-cutting government initiatives are at risk in the appropriations process, but can still be salvaged:

Department of Commerce

- $5 million at the National Institute for Standards and Technology (NIST) to establish an expert security review team to help agencies review their systems and programs, identify unacceptable risks, and assist in mitigating them. This program would operate in the context of NIST's statutory responsibilities under the Computer Security Act of 1987 and Clinger-Cohen Act of 1996 to issue security guidance to the agencies.

- $50 million to create the Institute for Information Infrastructure Protection at NIST. The Institute would work collaboratively with industry and academia to fill research and development gaps for key security technologies. Industry often has no incentive to invest in long-term research and development without a clear market need. Research would be performed at private corporations, universities, and non-profit research institutes.

General Services Administration

- $5.4 million to maintain the Federal Computer Incident Response Capability (FedCIRC), the central government non-law enforcement focal point for responding to attacks, promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. A portion of this funding will also continue government support of Carnegie-Mellon University's highly acclaimed Computer Emergency Response Team (CERT).

- $10 million for next generation intrusion detection. This funding would be used to establish the Federal Intrusion Detection Network (FIDNet) which would complement FedCIRC by standardizing ongoing agency computer intrusion detection activities, automating many of the cumbersome manual processes now employed, and providing a centralized expert analytic capability that does not exist at most agencies.

Department of Treasury

- $7 million at Treasury to complete the development of an interoperable government-wide infrastructure to permit authenticated electronic transactions and thus promote the electronic delivery of services to the public. In our traditional, paper-based world, government, industry, and the public rely on trusted and verifiable relationships, photo IDs, notarized signatures, and face-to-face contact to authenticate one another's identity prior to conducting business. We need a similar authentication capability in our new electronic world. This funding would translate paper-based relationships into similar trusted and verifiable electronic relationships.

Office of Personnel Management and the National Science Foundation

- $7 million at the Office of Personnel Management and $11.2 million at the National Science Foundation for Federal Cyber

Services/Scholarships for Service. The Scholarship for Service effort will help develop the next generation of Federal information technology managers by awarding scholarships for the study of information assurance and computer security in exchange for Federal Service.

OMB's Role in Government Computer Security

In February, OMB Director Jacob Lew issued important guidance to the agencies on incorporating security and privacy requirements in each of their FY 2002 information technology budget submissions. In the future, when requesting approval for information technology funds, agencies must demonstrate how they have built adequate security and privacy controls into the life-cycle maintenance and technical architectures of each of their systems. Without an adequate showing, the systems will not be funded.

Let me use this point to illustrate OMB's role in computer security and put it in the context of today's hearing. While OMB does have a broad, government-wide role in formulating the President's budget, promoting the effective agency use of agency resources, and promoting sound agency management practices, including oversight of the use of agency information resources, our specific role for security is limited to policy development and oversight for unclassified government information and computer systems. We have no direct role in law enforcement or international affairs. While we maintain a close relationship with operational agencies, we have no operational responsibilities ourselves.

We are very much committed to the protection of Federal computer systems. We recognize that security, or information assurance as it is sometimes called, consists of a number of separate components:

- Confidentiality -- assuring that information will be kept secret, with access limited to appropriate persons for authorized purposes;

- Integrity -- assuring that information is not accidentally or maliciously altered or destroyed, that systems are resistant to tampering, and that they operate as intended;

- Availability -- assuring that information and systems will be ready for use when needed;

- Reliability -- assuring that systems will perform consistently and at an acceptable level of quality; and

- Authentication -- assuring that users of systems and parties to transactions are verified and known so that the sender knows that data has been delivered and the recipient knows the sender's identity. With authentication comes nonrepudiation, since neither party can later deny having sent or received the data.

The Legal Framework

Congress has provided a sound legal framework for the Executive branch to address computer security needs. OMB has built on this statutory framework. Relying on our general authority, we issued our first computer security policy in 1978. That policy defined a minimum set of controls for the security of Federal automated information systems tailored to the processing environment of its time -- a centralized environment running mostly custom-developed application software. In 1985, we updated that guidance as part of new, comprehensive guidance on information resources management, OMB Circular A-130. Appendix III of A-130, "Security of Federal Automated Information Systems," began to address the security vulnerabilities introduced by remote processing -- which at that time occurred largely through dial-up communications.

Today's computing environment is significantly different. It is characterized by open, widely distributed processing systems using commercial off-the-shelf software. While effective use of information technology often reduces risks to Federal programs (for example, reduced risks from fraud or errors), the risk to and vulnerability of Federal information resources has increased. Greater risks result from increasing quantities of valuable information being committed to Federal systems, and from agencies being critically dependent on those systems to perform their missions. Greater vulnerabilities exist because so many Federal employees have access to Federal systems, and because these systems now interconnect with outside systems and the Internet.

Two years after the issuance of Appendix III to Circular A-130, Congress enacted the Computer Security Act of 1987 (P.L. 100-235) requiring agencies to improve the security and privacy of Federal computer systems, plan for the security of sensitive systems, and provide mandatory awareness and training in security for all individuals with access to computer systems. The Computer Security Act established the National Institute for Standards and Technology (NIST) as having the lead in setting standards for the security of unclassified Federal information technology.

The Paperwork Reduction Act (PRA) of 1995, P.L. 104-13, then established a comprehensive information resources management framework which subsumed preexisting agency and OMB responsibilities under the Computer Security Act. It recognized our transition to an increasingly internetworked information environment, and the security and privacy challenges which go along with that transition.

OMB revised Appendix III to Circular A-130 in February 1996 to address specifically the computer security mandate of the 1995 PRA. The revised Appendix updated policies and set responsibilities for the security of Federal information systems including the confidentiality, availability, and integrity of information and systems.

Overall, OMB Circular A-130 sets forth government-wide polices for a wide variety of information and information resource management issues. The body of the Circular addresses agency management of information and information systems including capital planning and investment control. Appendix I sets privacy policy. The soon to be issued Appendix II defines policy for information architectures and implementation of the Government Paperwork Elimination Act. Appendix III sets security policy. In Appendix II -- our guidance on the Government Paperwork Elimination Act -- we address the authentication and nonrepudiation elements of security mentioned earlier.

Appendix III implements another Computer Security Act requirement by directing the Department of Commerce (through NIST) to issue appropriate security standards and guidance, update security training guidelines, provide guidance for security planning, provide guidance and assistance to Federal agencies on appropriate security when interconnecting with other systems, coordinate agency incident response activities, evaluate new technologies, and apprise Federal agencies of their security vulnerabilities.

Importantly, Appendix III also requires Federal agencies to adopt a minimum set of risk-based management controls. Four controls are described: assigning responsibility for security; security planning; periodic review of security controls; and management authorization. These controls are intentionally not technology dependent. Instead, they focus on the management controls agencies need to assure adequate security of the information technology now in the hands of millions of Federal users. Technical and operational controls should support these management controls.

More recently, the Information Technology Management Reform Act of 1996 P.L. 104-106 Div. E (Clinger-Cohen Act) linked OMB and agency computer security responsibilities firmly to agency information resources management, capital planning, and budget processes. It established agency Chief Information Officers who report to agency heads as the responsible focal point for agency information resources management, including security. Agency CIOs are responsible for oversight of the security policies and practices embodied in the Computer Security Act, the Paperwork Reduction Act of 1995, and OMB Circular No. A-130. These responsibilities include the need for explicit consideration of security requirements in the development of agency information technology architectures and the need to ensure appropriate levels of security awareness and training.

The Clinger-Cohen Act tied agency information resource management responsibilities, including security, to the capital planning and budgetary oversight process the agency engages in with OMB. When OMB reviews information technology investment plans generally, or when it examines specific major information systems, it evaluates agency security planning and practices. This reflects the influence of Clinger-Cohen.

Lastly, Clinger-Cohen recodified and highlighted Commerce's computer security responsibilities, particularly in the area of standards and guidelines. The Act underscored the requirement for agencies to ensure that their security planning was consistent with the standards and guidelines develcped by NIST. NIST issued comprehensive security planning guidance in December 1998.

In 1998, the Government Paperwork Elimination Act (the Paperwork Elimination Act) addressed OMB and agency responsibilities for conducting business in an electronic environment. It required that agencies provide for the optional use and acceptance of electronic documents and signatures, and introduce electronic record keeping when practicable. It provided that electronic records and their related electronic signatures must not be denied legal effect, validity, or enforceability merely because they are in electronic form. It also contemplated Federal acceptance of a range of electronic signature alternatives. By October 21, 2003, agencies must have electronic filing and electronic signature capabilities in place. OMB published its guidance on implementing the Act in the Federal Register on May 2nd 2000. The guidance describes the methods agencies can use to provide for the authentication of digital signatures.

Are current policies effective?

In reviewing our recent efforts in the area of computer security, OMB has taken a close look at the effectiveness of our current policies. In general, we believe that our policies and guidance for unclassified applications are adequate, although some updating and additional detail would be helpful. We plan to provide additional detail in our upcoming revision to these policies. Indeed, reports from GAO, including its assessment of security practices of leading private sector organizations, show that OMB policies and NIST guidance are properly focused on a risk-based, cost effective approach and reflect the right balance between strong security and mission needs.

As discussed earlier, OMB Circular A-130 establishes an overall framework for government information and information resource management. We must integrate security within this framework to ensure that it remains cost-effective, forms an integral part of agency business processes, enables rather than impedes agency missions, and operates effectively over time.

How can we ensure effective policies?

We recognize that security measures must function effectively in the real world of agency missions and business operations. To accomplish this, we focus on a number of key principles:

- We should consider widely diverse views and attempt to accommodate unique agency needs. Agency information management practices often affect the public, industry, and state and local governments. In considering new approaches to security we need an open and transparent process that encourages and makes good use of public comment.

- Although the views of the general security and national security community are essential in developing sound security policy, they are not the only ones we should consider. Agency CIOs, program officials, and others also have important perspectives and their views are essential in the policy development process.

- Ultimately, the responsibility for security of systems and programs should lie with each agency and with the specific program officials in each agency. Unless we develop policy that fits within that context, security will become an afterthought.

- Compliance always improves when we build security into our systems and work processes in close coordination with the program officials that are closest to the affected operations.

- Funding and managing security apart from a program encourages program officials, system owners and users to ignore it. Separation sends a signal to them that security is not their job. If program officials and users do not take responsibility for security, then security officers and others must do so, often by employing resource intensive compliance inspections. This approach carries risk since the only time one knows the level of compliance is during or immediately following an inspection.

Good design and good planning are the keys to successful security. They are the keys to successful security. For good design, security must be compatible with and enable -- not unnecessarily impede -- system performance, business operations, and the mission. When security unnecessarily slows the system or hinders the mission, users often work around it or ignore it completely. To work effectively, security must be part of the system architecture, built-in so that users will "buy-in."

Good planning requires that we fund security and privacy as part of the life-cycle costs for each system. To identify true system costs and adequately plan for future system or program operations, we must account for all of the resources necessary to operate the systems, including security. Indeed, attempting to fund security independent of the program or system within which it lives makes it far more difficult to build a business case for the security component. If it isn't tied to the mission, how can one demonstrate security's support of the mission?

Our approach provides maximum flexibility for agencies so that they can make appropriate, informed choices in applying necessary security controls that are consistent with their unique circumstances. It minimizes conflicts that could easily arise from any centralized approach to widely diverse agencies with a broad range of varied and shifting requirements.

How can we improve compliance?

As GAO, our agency Inspectors General, our own program reviews, and industry and private security experts all agree, most security problems come not from a lack of policy, but rather from ineffective or incomplete implementation of existing policies and guidance. We are very much aware of this risk in the Federal context. In government, ineffective implementation can arise from inadequate resources, lack of management attention, and inadequate employee training. In the past few years, a great deal of agency management attention focused on Y2K remediation, drawing on agency resources and delaying full implementation of the Clinger-Cohen approach. There is much more to be done before we reach full implementation of our existing security guidance.

We believe agencies must meet the following three goals to ensure successful security policy implementation:

- They must achieve consensus and get user buy-in when initially setting policy so that the product will be better.

- They must tie security to their capital planning and investment control process and to their budgets.

- They must establish and maintain senior management support.

OMB will do all that it can to encourage and help the agencies in these efforts.

To identify specific problems regarding implementation, we are collecting empirical data from the agencies. We began in June 1999 with a systematic review of agency risk management processes. We are now focusing on the security posture of 43 high impact government programs such as Medicare, Medicaid, the Air Traffic Control System, Social Security, and Student Aid.

Our findings to date are illuminating. Agencies need to improve their integration of security into their capital planning and investment control processes. As mentioned earlier, in February of this year, we provided the agencies with the first step towards a solution -- specific security criteria that agencies must meet before they receive FY 2002 funding for information technology investment requests. These criteria require agencies to demonstrate explicitly how their information technology investments provides for adequate security controls and how they account for the costs of those controls over the life of each system.

Additionally, OMB's budget preparation guidance to the agencies this year will add a requirement that they include, for each system, a percentage amount for security. Over time, we believe this will give us better information on true security costs.

Cross-Cutting Efforts

We are working with the NSC, the CIO Council, NIST, GSA, GAO, and others on a number of specific projects to assist the agencies and enhance government-wide security. These include:

- Testing a systematic process of identifying, assessing, and sharing effective security practices. The CIO Council has developed a searchable database and website to facilitate this activity.

- Finalizing security performance measures (metrics) against which agencies can assess their security programs and take steps to mature them over time. Agency comments on the final draft of this assessment framework are due this week. NIST and the CIO Council are scheduling a workshop for August to discuss the comments broadly. It is significant to note that our assessment framework compares favorably with the results of a similar effort by a major financial institution widely recognized as an industry leader in security.

- Creating a formal process for coordinating the government-wide response to cyber incidents of national significance. This process includes the formation of a working group consisting of OMB, the FBI, Departments of Justice, Defense, and Commerce, the intelligence community, GSA, and the CIO Council, along with a senior level steering group consisting of senior officials from the above agencies, the NSC and OSTP.

- Improving the operational effectiveness of the Federal Computer Incident Response Capability (FedCIRC) in responding to lower level incidents and coordinating federal agency sharing of information regarding common vulnerabilities and computer incidents. Several years ago, OMB designated FedCIRC as the primary avenue for agencies to fulfill their information sharing responsibilities. OMB and the CIO Council are working together to enhance that capability.

- Using the FedCIRC organization to promote more timely agency installation of patches for known vulnerabilities. Many successful attacks against government and industry systems have been the result of old vulnerabilities for which vendor patches are readily available at no cost. Installing such patches is not, however, a trivial task; it requires considerable time and effort on the part of systems administrators who often are busy just keeping their systems up and running efficiently. We hope to provide some relief through this cross-cutting initiative if we can obtain necessary future funding.

- Reviewing security policies and practices of the national security community to see if they have applicability for those agencies that operate in an unclassified environment. Where appropriate, those policies and practices will be adapted for general agency use.

- Exploring with the CFO Council the viability of establishing a security benchmark or standard expectation for the security of agency financial systems. This effort may prove to be an effective pilot for establishing similar benchmarks for other discrete classes of information and systems. At the same time, we want to move carefully in this area to avoid the temptation to establish one-size-fits-all security requirements.

- Developing a government-wide Public Key Infrastructure (PKI) - a trusted digital signature infrastructure that will facilitate a broad range of services including tax filings, regulatory submissions, student and small business loans, benefit applications, grants, and many more. The PKI will be essential to agency implementation of the Paperwork Elimination Act. The Federal PKI Steering Committee, sponsored by the CIO Council, is working with government agencies and industry to field a comprehensive network-based infrastructure to support a federal PKI. Part of this task involves allowing digital signatures from different government agencies and different vendors to interoperate. A pilot, "Certificate Bridge Authority" successfully tested this interoperability in April and will be operational later this year. The PKI, through digital signature services and encryption, provides four of the basic security services I mentioned earlier -- confidentiality, integrity, authenticity, and non-repudiation. For all of these efforts, adequate future funding will be essential.

These are innovative efforts that show great promise. They need Congressional support if we are to fulfill that promise.

New Legislation

On a current note, we are very supportive of the Government Information Security Act of 2000, now part of the pending FY 2001 Defense Authorization Act. The Administration worked closely, in a non-partisan way, with the authors of this legislation. We share a desire to meet the security needs of the government and promote security as an essential management function. The Federal government has come a long way since the original Computer Security Act was passed in 1987. There have been significant technology and policy changes along the way. If it becomes law, the Government Information Security Act will update our statutory framework in a thoughtful and constructive manner.

Conclusion

We appreciate your interest in all of these matters and look forward to continuing our close cooperation with the Committee in this important area. We value our partnership with you and hope that this hearing will mark a further strengthening of our joint efforts on behalf of the American people.

Thank you.

Mr. HORN. Thank you, Mr. Spotila. I would like to ask a few questions before you leave.

OMB Circular A–133, section 3, so forth, requires that agencies have an incident response capability to address security incidents in a system and to share information concerning common vulnerabilities and threats. The incident response capability shall share information with other organizations and assist the agency in pursuing appropriate legal action consistent with the Department of Justice guidance, is our reading of that.

Have all the agencies complied in developing an incident response capability?

Mr. SPOTILA. Mr. Chairman, to varying degrees, all of the agencies have sought to comply. One of the areas of focus, and I go into a little more detail in the written testimony, and we certainly would be happy to work very closely with you on this—that we in OMB have been focused on is how to get all the agencies to do a better job at this. And again some are better at it than others in the nondefense area.

We think that part of the answer is integrating it into their overall approach to information technology, not just an add-on, in other words, approach, but to integrate it into all of their planning. And although we are making progress, we also recognize there is much we need to learn, including how it is we assess how well they are doing. We are working with the CIO counsel and the agencies to develop popular metrics performance measures. We know there is a lot more work to be done here.

Mr. HORN. Are all agencies fully participating in the sharing of information on shared threats and vulnerabilities?

Mr. SPOTILA. To my understanding, they all are. I am not aware of any that have resisted that, for example.

Mr. HORN. What, if any, guidance will OMB issue that outlines a framework for sharing such information in an international context? Is there some thinking going on that?

Mr. SPOTILA. We have discussions under way. I don't know that we have made a decision as to what type of guidance would be appropriate in the international context. Our focus has been clearly with nondefense agencies and our focus has been obviously threats can come from anywhere in the globe. We are aware of that. But in terms of communicating outward in the international context, I think that is something that remains to be discussed and we are open to suggestions from you if you think we should do more.

Mr. HORN. Are we looking at the Embassies to help in this regard? I know in some cases we have appropriate security people. Or are you thinking of doing that and/or also direct contact with our security people and a particular nation's security people?

Mr. SPOTILA. There is obviously here an area where the State Department has had a lead in terms of focusing on security, particularly relating to the Embassy, and the Defense and National Security Agencies have been addressing this for some time. One of the questions is whether there is more that needs to be done beyond that and, if so, to what extent OMB should issue guidance. I think this is an area where we need to work on it in a continuing way.

The threat is evolving. The nature of the technology is evolving, and I think that we need to continually look at whether there is more that should be done.

Mr. HORN. Well, as you have suggested here, the computer security policy development and oversight that OMB has, and I take it then will plan some policy on international information and sharing and coordination?

Mr. SPOTILA. I would be happy to get back to you, Mr. Chairman, with a written response if you like and could perhaps elaborate on this more.

Mr. HORN. That is fine. Does the FBI's Carnivore program provide information and data to the National Infrastructure Protection Center? I would like to ask you and Mr. Vatis where we are on that.

Mr. SPOTILA. Mr. Vatis is probably much more familiar with the details of that than I am.

Mr. HORN. So OMB has not really been involved with that? It has been left to Mr. Vatis's organization?

Mr. SPOTILA. We have not been directly involved in that to my understanding. We're aware of it now and I know that we have asked for further information on it.

Mr. VATIS. Mr. Chairman, the Carnivore technique and other methods for electronic surveillance are the province of the FBI's Laboratory Division. The NIPC is one of the consumers of those techniques, just as the Organized Crime Program, the Counterterrorism Program, etc., are users of that technique. And my understanding is that we have had a small number of computer intrusion cases that have used that technique through the Laboratory Division.

Mr. HORN. Before you leave, Mr. Spotila, I was obviously interested in the $1.8 billion last year and now $2 billion this year. Did representatives of the administration make their case before either the authorization committees or the appropriations subcommittees?

Mr. SPOTILA. My understanding is they have. And I think that some of these decisions remain out there in the initial markups. A number of these areas are not being funded, which has been raised certainly to a level of concern internally. Sometimes that reflects perhaps less of a willingness to deal with crosscutting initiatives that affect lots of agencies, particularly in a context of relatively lean resources at the subcommittee level.

This is a transition area. That is one of the reasons that I refer to it in my testimony. We are all in a position of change here and as we try to work with the agencies to look for crosscutting approaches, one of the realities is that the appropriations process is not always set up to look at it the same way.

We obviously have not been effective enough in making the case because the record thus far in terms of how the appropriations subcommittees are dealing with it is not as good as we would like it to be. But the process is not over, which is one of the reasons we wanted to call it to your attention as well.

Mr. HORN. I am delighted that you did. And if you want to give me a letter that I can play postage man with the appropriators, I would be glad to do it.

Mr. SPOTILA. Certainly, we will do that. We will followup with that.

Mr. HORN. Thank you very much and I know that you have——

Mr. SPOTILA. Thank you very much, Mr. Chairman. Thank you for your courtesy.

Mr. HORN. OK. Back to the regular order. Our next speaker has come a long way also, and that is Mr. Elfren Meneses, the Antifraud and Computer Crimes Division, National Bureau of Investigation of the Philippines. Mr. Meneses.

Mr. MENESES. Mr. Chairman, members of this committee, good morning. I am Elfren Meneses. I come from Manila, Philippines and am presently employed in the National Bureau of Investigation.

My agency is under the Department of Justice, and its history is that it started as a Division of Investigation in the Department of Justice and later on organized as the National Bureau of Investigation under Republic Act 157 in June 1947. Under the Republic Act 157, as amended, the NBI is empowered to investigate crimes and other offenses against the laws of the Philippines both at its own initiative and as public interest may require; to assist when officially requested in the investigation or detection of crimes and other offenses; to act as national clearinghouse of criminal records and other information for use of all prosecuting and law enforcement entities in the Philippines; to give technical help to all prosecuting and law enforcement officers, agencies of the government, and courts which may ask for its service.

Its added functions include to investigate Tanodbayan cases; to actively participate in the activities of the ICPO-Interpol; and to perform such other related functions as the Secretary of Justice may assign from time to time.

The NBI is composed of six services; namely, the Special Investigation Services, which is based in Manila and charged with the investigation of common crimes, heinous crimes, white collar crimes, and transnational crimes. The other services are the Regional Operation Service, the Domestic Intelligence Services, the Technical Services, the Administrative Services and the Controller Services.

The investigator in the National Bureau of Investigation is called an NBI agent with the qualification that he must be a member of the Philippine Bar or he must be a lawyer or a Certified Public Accountant. He must be between the ages of 24 and 35 years old and must not have a derogatory record.

On the issue of computer law of the Philippines, a week after the start of the investigation of the "ILOVEYOU" virus by the National Bureau of Investigation, the 11th Congress of the Republic of the Philippines and the Senate started reviewing pending bills in both houses. On June 14 of this year, President Joseph Ejercito Estrada approved Republic Act No. 8792, entitled "An act providing for the recognition and use of electronic commercial and noncommercial transactions, penalties for unlawful use thereof, and other purposes." It is also called as our E-commerce Act.

Prominent in this law is section 33 of Republic Act 8792 wherein it states: The following acts shall be penalized by fine and/or imprisonment, as follows: Hacking or cracking, which refers to unauthorized access into or interference in a computer system/server or information and communications system, or any access in order to corrupt, alter, steal or destroy, using a computer or other similar information and communication devices without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, attack or loss of electronic data, message, or electronic documents, shall be punished by a minimum fine of 100,000 pesos and a maximum commensurate to the damage incurred and a mandatory imprisonment of 6 months to 3 years.

Now, on the issue of international cooperation, the cooperation between the National Bureau of Investigation and the FBI Legal Attache in Manila in the investigation of cyber intrusion is excellent. Fast and constant exchange of information by both offices is always assured. Technical people from the FBI are immediately sent to the Philippines upon need to confirm evidence gathered by the NBI agents.

To update the NBI agents in their investigation of cyber intrusions, Legal Attache in Manila recommends the training of agents at the FBI Academy in Quantico, VA or any FBI-sponsored training conducted in the Philippines.

An example of this is the investigation of the “ILOVEYOU” virus wherein both offices, the NBI and FBI Legal Attache, worked closely from the startup to the termination of the investigation and even after the filing of the case before the Department of Justice of the Philippines.

Another example of cooperation by both offices is the arrest and deportation of U.S. fugitives in the Philippines. As of the end of June this year, there were 15 U.S. fugitives arrested, 13 of which were deported to the United States, two are still in the process of extradition.

At this point in time, we also coordinated during the Y2K millennium bug. And in line with its international relations, the NBI is actively participating in tracing perpetrators of cyber intrusions, as well as personalities known for bank fraud and other electronic commercial offenses. These efforts the NBI will continue to pursue as it honors its commitment to the global community.

At this stage I would like to thank you, Mr. Chairman, for inviting us here and to give our statement. Thank you very much.

[The prepared statement of Mr. Meneses follows:]

Republika ng Pilipinas
(Republic of the Philippines)
Kagawaran ng Katarungan
(Department of Justice)
PAMBANSANG KAWANIHAN NG PAGSISIYASAT
(NATIONAL BUREAU OF INVESTIGATION)
Maynila

Tanggapan [illegible]
(Office of the Director)

INTERNATIONAL CYBER CRIMES CONGRESSIONAL HEARING, WASHINGTON , D.C., JULY 24-27, 2000 REPRESENTED BY ATTY. ELFREN L. MENESES , DIRECTOR I, OF THE NATIONAL BUREAU OF INVESTIGATION, MANILA, PHILIPPINES

THE NATIONAL BUREAU OF INVESTIGATION (NBI)

The National Bureau of Investigation (NBI) saw its inception on November 13,1936 upon approval of Commonwealth Act No. 181 by the legislature. It was the brainchild of the late President Manuel L. Quezon and Jose Yulo, then Secretary of Department of Justice.

Tasked with organizing a division of Investigation patterned after the United States Federal Bureau of Investigation were Thomas Dugan, a veteran American police captain from the New York Police Department and Flaviano C. Guerrero, the only Filipino member of the United States Federal Bureau of Investigation.

On the basis of stiff physical, mental and moral standards, 45 men were selected as agents from among 300 applicants. To complement that investigative force was a civilian composed of doctors, chemist, fingerprint technicians, photographers, stenographers, and clerks.

During the Japanese occupation, the Division of Investigation (DI) was affiliated with the Bureau of Internal Revenue and the Philippine Constabulary known as the Bureau of Investigation (BI). Subssequently, during the post-liberation period, all available DI agents were recruited by the US Army CIC as investigators.

Since then, the Bureau assumed an increasingly significant role. Thus, on June 19,1947, by virtue of Republic Act No. 157, it was reorganized into the Bureau of Investigation. Later, it was amended by Executive Order No. 94 issued on October 4, 1947 renaming it to what it is presently known, the National Bureau of Investigation (NBI).

offices, [illegible]
services;

To extend its services in the investigation of cases of administrative or civil in nature in which the government is interested;

To established and maintain an up-to-date scientific crime laboratory and conduct researches in furtherance of scientific knowledge in criminal investigation;

To coordinate with other national or local agencies in the maintenance of peace and order;

To undertake the instruction and training of a representative number of city and municipal peace officers at the request of their respective superiors along effective methods of crime investigation and detection in order to insure greater efficiency in the discharge of their duties;

ADDED FUNCTIONS

To act as one of the law-enforcement agencies assigned to investigate Tanodbayan cases;

To actively participate in the activities of the I.C.P.O.-Interpol;

To operate and maintain the Tagaytay Treatment and Rehabilitation Center which constitute the nucleus of such centers as maybe created, authorized, and/or accredited under R.A. 6425(Dangerous Drug Act of 1972);

To perform such other related functions as the Secretary of Justice may assign from time to time.

ORGANIZATIONAL STRUCTURE AND JURISDICTION

The NBI is a government entity that is civilian in character, and national in scope. It is under the Department of Justice and headed by a director and supported by an Assistant Director and six(6) Deputy Directors for Special Investigation Services, Regional Operation Services, Intelligence Services, Technical Services, Administrative Services, and the Comptroller Services. Its central office is located along Taft Avenue, Ermita, Manila.

To give Technical help to all prosecuting and law enforcement offices, agencies of the government, and courts which may ask for its services;

THE "TWO PILLAR RULE"

THOROUGHNESS and LEGALITY - has always been strictly adhered to by the NBI in the investigation of cases.

The legality of the Bureaus activity is assured by its Legal and Evaluation Division, which is tasked with providing legal counsel to the Director, legal services to the Bureau, evaluate the investigation reports of the Agents, and conduct legal researches and studies.

SPECIAL INVESTIGATION SERVICES (SIS)

The SIS through its 11 Manila based investigative units, attends to various common crimes, heinous crimes, white collar crimes, and transnational crimes.

REGIONAL OPERATION SERVICES (ROS)

The Bureau has nationwide links with the citizenry. There are at present fifteen (15) regional offices and nineteen (19) district offices (then known as sub-offices which are extentions of regional offices).

DOMESTIC INTELLIGENCE SERVICES (DIS)

The Domestic Intelligence Services collects, analyzes, and interprets intelligence information relating to crime, criminals, and national security for the operational use of the Bureau and the intelligence community.

In collaboration with its foreign counterparts, it exchanges intelligence information that results to the prevention or solution of international crimes and in the apprehension of international criminals, terrorists, and fugitives.

As an adviser of the National Intelligence Board, it contributes and assist in the formulation of intelligence policies of the government and the drafting of appropriate strategies on national security.

TECHNICAL SERVICES (TS)

ITS OBJECTIVE

The main objective of the National Bureau of Investigation is the establishment and maintenance of a modern, effective and efficient investigative service and research agency for the purpose of implementing fully the principal functions provided under Republic Act 157, as amended.

ITS VISION

An institution that is reliable and dynamic in providing quality investigative and support services, by committed professionals, to serve the ends of truth and justice, founded on the fine ideals of Nobility, Bravery and Integrity.

ITS MISSION

To provide quality services for efficient law enforcement in the pursuit of truth and justice.

ITS FUNCTIONS

Under R.A. 157, as amended, the NBI is empowered

To investigate crimes and other offenses against the laws of the Philippines, both on its own initiative and as public interest may require;

To assist, when officially requested in the investigation or detection of crimes and other offenses;

To act as national clearing-house of criminal records and other information for use of all prosecuting and law enforcement entities in the Philippines, of identification records of identifying marks, charactristics and ownership or possession of all firearms and test bullets fired therefrom;

To give Technical help to all prosecuting and law enforcement offices, agencies of the government, and courts which may ask for its services;

The Technical Services provides technical assistance and expertise in scientific crime detection and investigation not only to its operating units (Investigative Services) but also to the local police agencies, fiscals, courts and other government or private offices that seek such assistance in the field of forensic chenistry, deoxyribonucleic acid (DNA), medicine, ballistics, questioned documents, polygraph, dactyloscopy, photography, and criminal records and identification.

Per established policy of the Bureau, pursuant to the provisions of Section 1 (c and d) of R.A. 157, as amended, NBI records and information, as well as technical services, may be availed of only by law enforcement and prosecuting agencies, the courts and other government offices in connection with cases under investigation or adjudication, or for other official purposes.

The Technical Services branch, however, may accommodate requests for technical assistance by private parties if properly coursed through the government agency concerned.

There is, however, an exception to the rule on technical assistance. Request for autopsy cases are filed directly with, and attested to, by the NBI.(No fee is charged by the NBI in all autopsy service cases). All investigations handled by the NBI automatically include its technical aspect.

The Bureau through its Identification and Records Division serves as the national clearing house and repository of all criminal and other information that are of interest and concern to law enforcement, the administration of justice, and national security.

As such it keeps and maintains a systematic centralized file of the names and fingerprints of persons involved one way or the other in criminal offenses in any part of the country, including a representative number committed abroad, and the personal identification records of aliens, and citizens that are non-criminal in nature.

ADMINISTRATIVE SERVICES (AS)

The Administrative Services extends its support to the other branches of the Bureau in relation to personnel, supplies and equipment, information, records and other administrative matters. These tasks are being rendered by the following divisions: General Services, Personnel, Information, Statistics, and Focal Point for Gender Concerns.

COMPTROLLER SERVICES (CS)

The Comptroller Services is charged with matters relating to budget, accounting, management/planning and audit. These tasks are handled/performed by the Budget, Accounting, and Management, Planning and Audit divisions.

THE NBI AGENT

The qualification for the position of an Agent are:

1. The applicant must be a member of the Philippine Bar (or a certified public accountant), of good moral character, and of excellent physical and mental condition;

2. Must be between the ages of 24 and 35 years, weigh not less than 125 lbs. and at least 5'5" in height;

3. Must not have a derogatory record.

An NBI Agent is identified through an identification card he/she carries as an agent of the NBI. It bears the agent's name, signature, photograph, blood type, and the signature of the Director. With the ID goes a badge bearing the NBI seal and indicating the agent's rank.

NBI agents pass through rigid screening and undergo extensive training at the NBI Academy. Those who pursue further training are sent to prestigious institutions in police science and administration, like the Scotland Yard in England; the Federal Bureau of Investigation (FBI) in the United States; the Royal Canadian Mounted Police (RCMP) in Canada; and in similar schools in Australia, Japan and other foreign countries.

As a policy, an NBI agent is trained to use firearms only in self-defense, or to safeguard the lives of other persons.

There are lady agents among the ranks of NBI investigative personnel, who, like their male conterparts, undertake the manifold aspects of crime detection and investigation.

Law is a desirable qualification for agents because in addition to having knowledge of the elements of crimes and the rights of suspects, agents must be able to collect legally admissible evidence in the course of a criminal investigation.

On the other hand, Accounting can be an alternative educational qualification, because expert knowledge of accounting practices and procedures is required in the investigation of various cases under the jurisdiction of the NBI such as frauds, illegal business manipulation, and other white-collar crimes.

DRUG TREATMENT AND REHABILITATION CENTERS

In the relentless drive against drug dependency, the NBI maintains drug treatment and rehabilitation centers.

The Treatment and Rehabilitation Center (TRC) was established in Tagaytay City upon the creation of the Bureau's anti-narcotics section in January 1965. Its main objective is "to provide an adequate and effective treatment and rehabilitation program for drug dependents.

It has also a drug treatment and rehabilitation center in Cebu City to serve drug dependents in the area. It is known as The New Horizon located at the Boy Scouts of the Philippines (BSP) grounds, Capitol Hills, Cebu City and started operations on December 16, 1984. It is administered by the NBI having full responsibility for funding technical personnel and administration.

The thrird drug treatment and rehabilitation center is in Cagayan de Oro City. It serves the constituents who need our services in Mindanao.

PROCEDURES IN APPLYING FOR AN NBI CLEARANCE

One may secure an NBI clearance by appearing at the NBI office in Manila and following the procedures, namely: payment of fee, filling-up of form, picture-taking, fingerprinting, and registration.

On the date of release of the clearance certificate, the applicant returns to the NBI and presents the receipt to the Releasing Section where the clearance certificate is issued.

A clearance applicant in the provinces can also apply through the various NBI regional and district offices. The same basic procedures in clearance application in Manila are followed.

The Bureau has also satellite offices for the purpose of NBI clearances such as in Quezon City, Mandaluyong City, Caloocan City, Pasig City, Camp Crame (Q.C.), and Trece Martirez City (Cavite).

CIRCUMSTANCES UNDER WHICH THE NBI MAY BE CONTACTED

When a crime has been committed or is about to be committed, any aggrieved person may seek NBI assistance. Any person possessing valuable information in connection with any violation of the Philippine laws is welcome at any NBI office if he is willing to furnish the Bureau with said information.

Those who may wish to file their complaints in Manila, may go directly to the NBI Complaints and Recording Division (CRD) and file his/her complaint under oath. Walk-in complainants in filed offices may see the chief or any agent thereat for purposes of filing his/her complaint.

When the aggrieved party cannot personally undertake this, a letter addressed to the NBI Director containing the said complaint shall suffice.

The NBI in some instances, may be called to attend to criminal cases already under investigation by the local police. However, the requesting party or aggrieved party shall so state in the complaint dissatisfaction over the handling of the case, and/or upon directive from higher authorities.

All forms of assistance extended by the NBI to other government institutions as well as to the private sector are ABSOLUTELY FREE.

COMPUTER CRIME LAW OF THE PHILIPPINES

A week after the start of the investigation of the "I LOVE YOU VIRUS" by the National Bureau of Investigation, the Eleventh Congress of the Republic of the Philippines and the Senate started reviewing pending bills in both Houses. On June 14, 2000 President JOSEPH EJERCITO ESTRADA approved Republic Act No. 8792 entitled AN ACT PROVIDING FOR THE RECOGNITION AND USE OF ELECTRONIC COMMERCIAL AND NON-COMMERCIAL TRANSACTIONS, PENALTIES FOR UNLAWFUL USE THEREOF, AND OTHER PURPOSES or Otherwise known as the E-COMMERCE ACT.

The said Act is a consolidation of Senate Bill No. 1902 and House Bill No. 9971 which was finally passed by the Senate and the House of Representatives on June 8, 2000 and June 7, 2000, respectively.

SEC. 33 of R.A. 8792 Provides, Penalties. - The following Acts shall be penalized by fine and/or imprisonment, as follows:

a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system, or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents shall be punished by a minimum fine of One Hundred Thousand Pesos (Php100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six(6) months to three (3) years.

INTERNATIONAL COOPERATION AND CASE EXAMPLES

The cooperation between the NBI and the LEGAT, Manila in the investigation of cyber intrusions is excellent.Fast and constant exchange of information by both offices is always assured. Technical people from the FBI are immediately sent to the Philippines upon need, (to confirm evidence gathered by NBI Agents).To update NBI Agents in the investigation of cyber intrusions, LEGAT, Manila recommends the training of Agents at the FBI Academy in Quantico, Virginia or FBI sponsored training conducted in the Philippines.

An example of this is the investigation of the "I LOVE YOU virus", wherein both offices (Legat and NBI) worked closely from the start up to the termination of the investigation, and even after the filing of the case before the Prosecutors Office .

Another example of cooperation by both offices is the arrest and deportation of US fugitives in the Philippines. As of the end of June 2000, there were 15 US fugitives which were arrested in the Philippines, 13 were deported to the United States of America. Two (2) are still in the process of extradition.

At this point in time both offices are monitoring significant developments that may occur relative to the Y2K Millenium Bug inthe Philippines speecially on banking institutions.

In line with its international relations, the NBI is actively participating in tracing perpetrators of cyber intrusions, as well as personalities known for bank fraud, and other electronic commercial offenses. These efforts, the NBI will continue to pursue, as it honor its commitment to the global community.

Mr. HORN. We definitely appreciate all you have gone through and we are delighted to have you share those experiences with the rest of us. So we will get to some of that more in the question period.

We will now go to Mr. Ohad Genis, advocate, chief inspector National Unit for Fraud Investigations, Israeli Police. Welcome.

Mr. GENIS. Good morning and shalom to everyone. And by the way it is Genis, not Jenis.

On behalf of the Israel Police, I would like to thank you for this tremendous opportunity to appear before you and discuss our point of view concerning cyber crime and international cooperation. Of the 50 cyber crime cases dealt with by our department, 20 cases had an international component.

I would like to stress that our department does not handle all the cyber crime cases in Israel. Cases that are of local interest or that do not require intensive organization are done by the field units and, unfortunately, I don't have their data. However, I can estimate that more than 30 percent of our cases require international cooperation and there is definitely a growing number of cases—of requests, sorry, for international assistance.

In the global arena when referring to the Internet as a borderless scene of a crime, an effective international cooperation is the key to success. And when I say effective, I mean both the accuracy of the data received from abroad and the time it takes to be transferred.

Today, all of the Israel ongoing cooperation is with the United States, which we warmly welcome since you always deliver the goods with the help of the great and most efficient legal attaches in Israel, Special Agents Kerry Gleicher and Scott Jessey, and we enjoy an excellent working relationship with the FBI.

However, during an investigation when we are obliged to request for international assistance, due to the complexity of the legal process, we know for sure that we have lost the time momentum and that the entire investigation will be put on hold for weeks and sometimes for months until we receive the relevant information, and I'd like to elaborate briefly on that.

We all know that in order to transfer data from one computer to another we must use a protocol, and the protocol used on the Internet is the Transmission Carrier Protocol, known as the TCPIP. This protocol identifies each and every computer connected to the Internet by a number called IP address, Internet Protocol address. And theoretically, each and every computer connected to the Internet receives a unique IP address.

We all use this IP address to trace our suspects. And most of our requests are for the identity of the user who used this specific IP address, or what was the IP address used by the user who sent a specific e-mail message.

For this data we still have to wait weeks and months and we believe that what is required today is the establishment of a central organization which will handle all requests for international assistance with on-line access, which will accelerate all the legal process—all the process of requesting international assistance.

Another matter that I'd like to mention is conducting international conferences. International conferences have proved themselves as being most efficient in all aspects of international cooperation, including sharing of experience, views and assumptions of solutions to common problems, etc. I had the privilege of participating in a conference held at the FBI Academy in March this year, and I can state categorically that our investigations have—our investigations benefited significantly from that conference in many aspects.

I would also like to mention that most of the foreign investigators, including the FBI investigators, felt that meeting face-to-face would assist us in our future cooperation.

I'd like to mention the time it takes for us to receive requested assistance from abroad now can be used by the hackers and they can to their advantage gain from this complication of law enforcement and use it to their own benefit, where in these investigations the time is of the essence.

In summation, I would like to say that in the high technology era, the establishment of an international center that would handle requests—international requests with on-line access and conducting international conferences and trainings would be the key to a successful joint effort in fighting cyber crime.

Thank you very much.

[The prepared statement of Mr. Genis follows:]

משטרת ישראל

Sunday 23 July 2000

Israel Police
Written Statement for the Congress of the United States, Committee on Government Reform

1. Description of the Agency:

The Israel Police is a national police force headquartered in Jerusalem and headed by a commissioner selected by the Minister of Internal Security. There are six districts (North, South, Tel Aviv, Jerusalem, Central, Judea/Samaria), three national investigative units (National Unit for Severe and International Crime, National Unit for Fraud Investigations, and, National Unit for Combating Car Theft), and the Border Patrol. The Israel Police was established on 14 May 1948, and currently employs 25,000 police officers.

The National Unit for Fraud Investigations, investigates white-collar crimes (WCC) committed by public sector employees; computer crimes of a public nature; and, crimes perpetrated via the Internet.

The National Unit established a computer crime squad, and
The crimes handled by this squad are complex computer crimes or those of a sensitive public nature, such as:

(a) A crime involving the defense establishment or senior public figures;

(b) A crime involving persons from abroad – penetrating Israeli computers from abroad and vice versa;

(c) The criminal activity effects the whole country rather than a city or region;

(d) Classic WCC crimes – bank fraud, forgery other economic crimes;

(e) Threats against public figures and government officials via the Internet;

(f) Publication of classified material to the public without prior approval via the Internet;

The computer crime squad is also responsible for providing technical and professional support in extracting evidence from computers seized from suspects during investigations by the Israel Police and other law enforcement bodies (i.e. Income Tax Authorities, Securities Commission, etc.). The computer squad also provides computer training to Israel Police officers.

2. Discussion of Computer Crime Law

In 1995, the Knesset, Israel's Parliament, reacted to a burgeoning increase in criminal activity through use of the Internet and enacted Computer Law that relates to the following subjects:

Article 1: defines the computer, data, output, programs, etc.;
Article 2: relates to obstruction, interference of computer programs and software;
Article 3: relates to false information or false printouts;
Article 4: relates to unlawful access to computer data;
Article 5: relates to intrusion into computer data in order to commit an additional offence;
Article 6: relates to the preparation and distribution of computer viruses ;
Article 7: defines damage liability for criminal computer crimes;

3. International Cooperation

In March 1998, the National Unit for Fraud Investigation encountered its first request for international assistance on a cybercrime matter. The State of California, U.S. Department of Defense (DoD) and U.S. Department of Justice contacted the Israel Police after detecting several successful intrusions into DoD, NASA and other commercial and academic computer systems. Preliminary investigation identified the criminal activity was emanating from Israel.

The Israel Police, working in close concert with U.S. investigators, identified the intruder and developed sufficient probable cause to request a search warrant. On 18 March 1998, the Israel Police seized a computer and other relevant materials from the suspect's home and conducted an extensive interview. Based on the investigative efforts in

Israel and the U.S., five Israeli citizens were indicted on 9 February 1999.

This investigation, known in Israel and the U.S. as the "Analyzer Case," received extensive media scrutiny in both countries. The main defendant will stand trial in Israel in the summer of 2000 and several U.S. law enforcement representatives will be witnesses on behalf of the Israeli government.

Cooperative efforts with the U.S. continue to this day and there are a growing number of requests for assistance on cybercrime matters from Israel to the U.S. and vice-versa. Based on the political climate in Israel, and the recent peace process negotiations with the Palestinian Authority and other Arab countries, the Israel Police continuously receive information that there are Internet sites that call for the assassination of Prime Minister Ehud Barak and other government officials. The Israel Police request that U.S. law enforcement authorities identify the person responsible for these threats and contact the webserver to see if this site violates a user agreement and remove it from the server.

The vast majority of requests from U.S. law enforcement continue to be in the area of computer intrusions emanating from Israel. Generally, the Israel Police attempt to identify the person(s) responsible for this activity and coordinate investigative strategy.

Mr. HORN. We thank you very much. That's very helpful case study.

We now go to Mr. Edgar A. Adamson, the Chief of the U.S. National Central Bureau, Interpol. Thank you for coming.

Mr. ADAMSON. Mr. Chairman, thank you for providing me the opportunity to participate in today's subcommittee hearing on computer security issues. I am currently assigned to the position of Chief of the U.S. National Central Bureau of Interpol. I am a U.S. Treasury Special Agent with 30 years of experience with the Customs Service Office of Investigations. The Interpol U.S. National Central Bureau is a component of the Department of Justice with representatives from 16 different U.S. Federal law enforcement agencies, including a management team from both the Department of Justice and the Department of Treasury.

As you are well aware, the information revolution has changed the world forever, transforming the way we think and the way we use information. Our dependence on these new sources and methods grow daily, and at least some part of nearly every interaction we undertake now occurs within this virtual world. Of course, this widespread dependence increases our vulnerability to criminal activity.

The ease with which criminals can access the means necessary to commit cyber crimes, the multiple jurisdictions in which these crimes are committed and the lack of adequate legislation for computer-related crime and the seemingly risk-free environment for the cyber crime perpetrator are all factors that point to a likely increase of this type of crime in the future.

Cyber crime is truly international in character as the electronic frontier has no bounds. It demonstrates that the need for international law enforcement cooperation has never been greater. To respond effectively, the U.S. law enforcement authorities must be able to overcome some very real cultural, linguistic, legal and digital barriers that complicate the positive exchange of criminal investigative information across national administrations and sovereign boundaries.

Interpol exists to facilitate this critical exchange among its 178 member countries and provides the necessary framework, rules of police cooperation, and essential tools and services that promote the adoption and use of international standards, foster best practice, and permit investigative results.

Interpol recognizes the severity of the cyber crime challenge and is committed to achieving effective computer security and cyber enforcement through the development and delivery of operational programs and training and the establishment of international standards and the promotion of best practices worldwide.

Interpol is in the unique position to facilitate timely and reliable notification concerning intrusion attempts and information on the widespread computer viruses through its worldwide communications network. The strength of the Interpol organization lies in the frame of law enforcement information exchange.

Interpol has established rules for police cooperation in its 178 countries. Interpol has been around for 75 years. It is the only global police organization. Worldwide on-line communications network links its membership. It is reliable, immediate, global, and it overcomes all the cultural, linguistic, and legal barriers.

The Interpol organization participates with other international organizations and national regional bodies. It participates and is a member of the G–8 Subgroup on High-tech Technology. It participates in the Council of Europe, and has observer status at the United Nations.

Regarding cyber crime, Interpol is a means again as to whereby we can exchange information on the varieties of cyber crime. We have a point of contact in all countries for immediate notification of security computer alerts, etc. We again work with the G–8 High-tech Subgroup. We coordinate training programs and we have various neutral forum meetings to develop best practices.

In recent years, the United States has made a strong commitment to Interpol. The U.S. Customs Commissioner Raymond Kelly has served for the last 3 years as Vice President for the Americas on Interpol's 13-member guiding Executive Committee, and FBI Deputy Director Tom Pickard has announced his intention to continue U.S. leadership in the organization and will stand for election to the Interpol Executive Committee this November.

Also this November, Ronald K. Noble will become the first non-European and the first American to hold the position of Interpol General Secretary—Secretary General in Lyon, France for a 5-year term. His candidacy was strongly supported by the heads of U.S. law enforcement organizations and prevailed on a platform of change to realize the organization's full potential. His vision for Interpol advocates greater inclusion for all its member nations and better use of electronic communication tools to increase the speed, accuracy and reliability of law enforcement exchange.

In conclusion, Interpol membership and participation increases the likelihood for detection, timely notice and law enforcement response to cyber intrusions. It also permits access to a 24-hour network of international experts and over 40 countries in a secure and confidential manner. Our ability to deal effectively and efficiently with cyber crime can be enhanced through competency building for less experienced enforcement agencies worldwide and through continued coordination and cooperation among U.S. law enforcement agencies dealing with various aspects of this emerging crime area.

I thank you again for permitting me the opportunity to address the subcommittee, and I am happy to answer any questions.

[The prepared statement of Mr. Adamson follows:]

TESTIMONY

of

Edgar A. Adamson
Chief
U.S. National Central Bureau – INTERPOL

before a hearing
of the

Subcommittee on Government Management,
Information, and Technology

July 26, 2000

"Cyber Crime – Computer Security"

Mr. Chairman and Members of the Subcommittee:

Thank you for providing me this opportunity to participate in today's Subcommittee hearing on computer security issues. I am currently assigned to the position of Chief of the United States National Central Bureau (USNCB) for INTERPOL, and possess thirty years of law enforcement experience as a Special Agent of the U.S. Customs Service. The USNCB is a component of the Department of Justice, with representatives from 16 U.S. federal law enforcement agencies, including both the Department of Justice and the Department of Treasury.

As the Members are well aware, the 'Information Revolution' has changed the world – providing unparalleled growth for our economy, and forever transforming the way we think about and use information. Our dependence on these new sources and methods grows daily – and at least some part of nearly every interaction we undertake now occurs within this 'virtual' world. Of course, this widespread dependence increases our vulnerability to criminal activity. The ease with which criminals can access the means necessary to commit cyber crimes, the multiple jurisdictions in which these crimes are committed, and the seemingly risk-free environment for the cyber crime perpetrator, are all factors that point to a possible increase in this type of crime in the near future.

Cyber crime is truly international in character, as the electronic frontier has no bounds. It demonstrates that the need for international law enforcement cooperation has never been greater. To respond effectively, U.S. law enforcement authorities must be able to overcome the very real cultural, linguistic, legal and digital barriers that complicate the positive exchange of criminal investigative information across national administrations and sovereign boundaries. The International Criminal Police Organization, INTERPOL, exists to facilitate this critical exchange among its 178 Member Countries, and provides the necessary framework, rules of police cooperation, and essential tools and services that promote the adoption and use of international standards, foster best practices, and permit investigative results.

INTERPOL recognizes the severity of the cyber crime challenge and is committed to achieving effective computer security and 'cyber enforcement' through the development and delivery of operational programs and training, the establishment of international standards, and the promotion of best practices worldwide. INTERPOL is in a unique position to facilitate timely and reliable notification concerning intrusion attempts, and information on the spread of computer viruses, through its worldwide communications network.

The role of INTERPOL, and particularly that of the USNCB, is often misunderstood. Before further describing INTERPOL's activity in the area of IT crime, I would like to take this opportunity to briefly present the Organization's structure and mission. INTERPOL officials are not James Bond-like detectives traveling the globe investigating crime. Instead, they assist operational efforts in each Member country by facilitating requests for criminal investigative assistance, and by providing expertise in a number of specific crime areas.

INTERPOL is the only global police organization. It is an inter-governmental alliance formed by 178 member countries for the purpose of exchanging criminal police information to combat ordinary law crimes and to support the U.N. Declaration of Human Rights. INTERPOL is recognized by, and cooperates with, other leading international organizations including the United Nations, the World Customs Organization, the Council of Europe and the Organization of American States. The Organization works closely with the G-8, and with many non-governmental and private organizations with mutual interests in law enforcement issues and crime prevention.

U.S. representation to the INTERPOL organization is coordinated through the U.S. National Central Bureau, or USNCB. Sixteen federal and state law enforcement agencies participate at the USNCB – and their officers bring to bear literally hundreds of years of collective investigative experience across the entire spectrum of criminal enforcement, and specific expertise in the conduct of international criminal investigation. The USNCB does not compete with U.S. federal agency attachė programs; rather it complements them.

The United States has made a strong commitment to INTERPOL. U.S. Customs Commissioner Raymond Kelly, has served for the last three years as Vice President for the Americas on INTERPOL's guiding Executive Committee. And FBI Deputy Director Thomas Pickard has announced his intention to continue U.S. leadership in the Organization, and will stand for election to the INTERPOL Executive Committee this November.

Also this November, Ronald K. Noble will become the first non-European, and first American, to hold the position of INTERPOL Secretary General. His candidacy – endorsed by the Attorney General and supported by the heads of U.S. federal law enforcement – prevailed on a platform of change to realize the Organization's full potential. His vision for INTERPOL advocates greater inclusion for all Member Nations and better use of electronic communication tools to increase the speed, accuracy and reliability of law enforcement exchange.

All 18,000+ U.S. law enforcement agencies – federal, state and local – may rely upon INTERPOL and the USNCB, to obtain needed intelligence and investigative assistance on computer security, and on all the variant flavors of cyber crime.

The INTERPOL Organization, and the USNCB, are involved daily in responding to requests for criminal investigative assistance on computer crime – traditional crime facilitated by information technology – such as child pornography, pedophilia, identity theft, and credit card fraud. And although its officers are not operational *per se*, INTERPOL is prepared to assist in the investigation of crimes against systems and networks, such as web site attacks and the malicious spread of viruses, and to help to sift through the thorny issues of jurisdiction and venue.

INTERPOL has taken an important role in coordinating worldwide law enforcement efforts in the area of IT Crime. Since 1990, the Organization has convened field experts for the purpose of sharing criminal investigative information, and developing international standards, best practice and training modules for the international law enforcement community.

There are currently four regional 'INTERPOL Working Parties on IT Crime' that meet regularly to deal with cyber crime issues. These fora provide unique opportunities for intelligence sharing and networking for experts in this rapidly advancing field. Recently, INTERPOL's 'European Working Party on IT Crime' developed and implemented a 24-hour early warning system that has been endorsed by the G8 Sub-Group on High Tech Crime.

INTERPOL collaborates closely with a number of organizations, academic and other, involved in projects to collate and evaluate national legislation on computer crime. Their aim is to ultimately develop international standards and best practice measures in the area of cyber crime. One example of this is INTERPOL's work with the Council of Europe to develop a draft convention on cyber crime. Provisionally entitled "Draft Convention on Cyber-Crime", this Council of Europe text will be the first international treaty to address criminal law and procedural aspects of various types of offending behavior directed against computer systems, networks or data, as well as other similar abuses. This text aims to harmonize national legislation in the field, facilitate investigations and allow efficient levels of cooperation between the authorities of different States. The text should be finalized by a group of experts by December 2000 and the Committee of Ministers could adopt the text and open it for signature as early as Autumn 2001.

INTERPOL is currently finalizing a cooperative agreement discussing coordination with the G-8 Sub-group on High-Tech Crime, aimed at preventing duplication and the resulting waste of resources.

INTERPOL works to promote awareness, education and the exchange of information in the area of cyber crime. In 1999, it revised and distributed 'Computers and Computer Crime', a computer crime manual of best practices for the experienced investigator. A handbook on computer-related crime for the novice investigator has also been published and distributed to all 178 INTERPOL member countries. INTERPOL will also shortly make information on IT crime matters available to law enforcement agencies and the public through its secure website.

The Organization hosts an annual conference to address IT topics such as internet investigations, e-commerce, digital evidence, tools and techniques, hacker profiling, internet legislation, encryption, and security matters.

INTERPOL also expends significant resources towards competency building in cyber crime investigation among its 178 Member countries and at regional levels. Teaming experts from highly advanced nations with those requiring the basics of investigative and forensic techniques has proved useful in raising awareness and knowledge among law enforcement throughout the world and ensuring that law enforcement entities can work together in this inherently international crime area.

Given the fast pace of cyber technology and the far-reaching effects of its criminal misuse, INTERPOL recognizes the need to cooperate efficiently and effectively with other international organizations and academic institutions with an interest in the field. It has, therefore, forged strong partnerships with bodies such as the G8 Sub-group on High Tech Crime, the International Chamber of Commerce (ICC), the Council of Europe, the United Nations Asia Institute for the Prevention of Crime and the Treatment of Offenders

(UNAFEI), as well as several academic institutions. This close collaboration helps to predict and prevent incidences of cyber crime by ensuring that timely information is shared and that existing resources are leveraged.

INTERPOL membership and participation increases the likelihood of detection, timely notice and proper law enforcement response to cyber intrusions. It also permits access to a 24-hour network of national experts in over forty countries, in a secure and confidential manner. Our ability to deal effectively and efficiently with cyber crime can be enhanced through competency building for less experienced enforcement agencies worldwide, and through continued coordination and cooperation among U.S. law enforcement agencies dealing with the various aspects of this emerging crime area.

Thank you again for permitting me the opportunity to address the Subcommittee. I am happy to answer any questions.

Statement: Atomic Tangerine - Interpol's position

The Interpol General Secretariat in Lyon was approached by a private company, Atomic Tangerine, with a proposal to explore the possibility of a co-operative approach to the prevention and detection of Internet crime.

Atomic Tangerine is a commercial consulting company based in Menlo Park, California, with other United States offices in Seattle, Boston, Washington, D.C., and overseas offices in London and Tokyo. It is related to Stanford Research Institute and funded by venture capital. This company has been vetted by the U.S. National Central Bureau, that is, the U.S. national Interpol office.

The current position is that there is no agreement, formal or informal, with this company. The two parties are exploring whether there may be viable possibilities for co-operation in this field. Any press reference to data collection, data exchange etc in no way relates to Interpol databases or police information processed on behalf of Interpol Member States by the General Secretariat.

Interpol considers that it is vital to protect the global business infrastructure on which all economies depend. Recognising that this infrastructure is at risk from high tech crime, and taking into account the extraordinary rate of development of this type of crime and the frontier-less environment in which it takes place, it is essential that the public and private sectors work together in strategic alliance to challenge cybercriminals in the most effective ways possible.

Interpol General Secretariat
19/7/2000

Subcommittee on Government Management, Information, and Technology
July 26, 2000
"Cyber-crime – Computer Security"

Response to Subcommittee Questions

1. **Can you estimate what percentage of your cases have an international component?**

100% of INTERPOL cases are international. INTERPOL is the only global police organization. It is recognized by, and cooperates with, other leading international organizations including the United Nations, the World Customs Organization, the Council of Europe and the Organization of American States. The Organization also works closely with many non-governmental and private organizations with mutual interests in law enforcement issues and crime prevention. Sixteen U.S. federal and state law enforcement agencies currently detail senior investigative staff to INTERPOL USNCB. Nine of these agencies also detail senior representatives to INTERPOL headquarters in France. All have gained from their investment in the form of increased international law enforcement cooperation and visibility.

As to the role of the U.S. National Central Bureau, it is an important component for U.S. participation in the INTERPOL network. As a condition of membership, each of INTERPOL's 178 Member Countries is required to establish and maintain a National Central Bureau (NCB) to serve as the point of contact for INTERPOL. NCBs are the operational organs of INTERPOL and the means through which the world's law enforcement entities exchange criminal investigative information and provide assistance. NCBs provide a single point of contact for domestic law enforcement components seeking assistance abroad, and for foreign governments trying to identify the authorities they need to contact in the United States.

The structure of U.S. law enforcement differs significantly from that of many INTERPOL countries, where size often dictates a single national police agency. By comparison, the multi-tier U.S. system – with more than 18,000 federal, state and local law enforcement agencies – appears large and fragmented, making it difficult for an outsider to know which department is empowered to deal with a particular matter or to supply information. Facts support this – as of 1998, there were over 83,000 sworn U.S. federal officers with arrest and firearms authority, with more than 50,000 engaged in criminal investigation, police and patrol activities. State and local law enforcement figures add to this complexity – as of June 1997, local police and sheriff departments numbered nearly 700,000 sworn personnel.

These U.S. officers are the USNCB's primary customers, and obtaining the international criminal investigative support they need is our primary mission. The same officers reciprocate with their international police colleagues by providing responses to foreign requests for investigative assistance forwarded from the USNCB – each request complying with U.S. laws and statutory authorities. This interaction with U.S. and foreign law enforcement – coordinating requests and responses for criminal investigative assistance (including translation support) – is the heart of the USNCB's daily business.

The USNCB is unique in U.S. law enforcement, and has been structured to meet the complexity of its mission. In addition to 65 permanent staff, the USNCB relies upon 23 detailed senior investigative staff from 16 U.S. federal and state law enforcement agencies to direct and coordinate domestic and foreign requests for criminal investigative assistance. It has also established a network of State police liaison offices in all 50 states to ensure the proper and timely receipt and response to investigative requests forwarded through state and local law enforcement channels.

As with other criminal matters, domestic law enforcement requests for assistance concerning computer related crimes, are forwarded to the appropriate INTERPOL member country; similarly, foreign requests for U.S. law enforcement assistance on international investigations are forwarded to the U.S. law enforcement component with statutory authority for the matter under investigation.

Unfortunately, statistics in the area of 'cyber crime', whether it be computer related crime, high tech or information technology (IT) crime are unreliable and at best incomplete, simply because the international law enforcement community is working with different definitions and legislation, where legislation is available. Currently, at least 60% of INTERPOL membership lacks the appropriate legislation to deal with Internet/computer-related crime. The result is that such offences are then classified according to their nearest common law derivative. For example, a case involving Internet related child pornography can end up being treated as an ordinary pornography or sexual offence statistic. Another problem is the lack of reporting by private firms due to a fear of the media/PR repercussions.

Regardless of our ability to account for every case of computer-related crime, our focus must be on its far-reaching potential for destructive criminal activity. The ease with which cyber crimes are committed, the multiple jurisdictions of these crimes, the lack of legislation, and the seemingly risk-free environment for the cyber crime perpetrator, are factors that point to a likely increase in this emerging crime type.

2. **How would you rate your cooperation with the Federal Bureau of Investigation's National Infrastructure Protection Center (FBI/NIPC) on cyber intrusion cases?**

   The USNCB cooperates with FBI's NIPC by routing inquiries for criminal investigative assistance it receives from foreign law enforcement components to that FBI unit for resolution. To date referrals to the NIPC on intrusion cases have been limited to a handful of cases.

3. **Could you comment on any past investigations which you worked with the FBI/NIPC?**

   The USNCB has cooperated with the NIPC by forwarding international requests for criminal investigative assistance on cyber crime. Typically, forwarded matters are then resolved by investigating offices who work directly with the requesting country. On the limited number of referrals made to NIPC, we have not received feedback on the final outcome of cases, nor have we received further inquiries from requesting countries indicating that issues were not appropriately handled by NIPC. We are currently exploring new ways of improving cooperative efforts with NIPC.

4. **What measures would be useful to you as investigators regarding record keeping by Internet Service Providers or by victims or cyber intrusions?**

   Because the USNCB is not operational, the actual investigative agencies handling INTERPOL referrals and collateral requests would in a better position to respond to this question. However, through experience gained in working with those agencies, we have noted that investigations are often hampered due to a lack of access to ISP records and transaction logs, or the inadvertent destruction of those records before law enforcement can gain access. Therefore, complete access to those records, authorized by warrant or subpoena, and more stringent record keeping legislation for ISPs, would significantly aid the investigator and help to assist in violator identification.

5. **Regarding training, what training can be done on a national or international basis to improve international response to cyber intrusions?**

   Because of the rapid growth in technology and its expansion to all sectors of society, cyber crime requires an appropriate and concerted effort from U.S. and international law enforcement. U.S. police and agent training courses should include introductory segments familiarizing personnel with cyber crime *methods and the general conduct of relating investigations, to include general computer forensic practices and rules on the handling of computer-related evidence. In addition, advanced courses should be made available to all requesting local, state and federal law enforcement agencies on specific cyber crime areas, and on complex relating matters, such as jurisdiction determination. This type of preparation will help ensure the enforcement response is adequate to the threat.*

Given the inherent international nature of cyber crime activity, law enforcement entities should also be familiar with the INTERPOL network and tools available to link them with the appropriate foreign law enforcement entities quickly and securely. In the area of IT crime, for example, INTERPOL maintains a 24-hour point of contact network comprised of approximately 40 member countries, accessible in each member country through its INTERPOL National Central Bureau. Department of Treasury and Justice new agent training programs now include a mandatory block of INTERPOL training, which introduces new agents to the techniques and strategies in conducting investigations with an international nexus, as well as tools available through the Organization. In the U.S., the USNCB State and Local Liaison Office offers basic INTERPOL training to state and local enforcement entities. Unfortunately these local training programs are heavily dependent upon dwindling financial resources that severely impedes our ability to reach a growing number of state and local police forces.

INTERPOL Headquarters in Lyon, France offers a number of training courses on information technology crime, such as "Computer-based Evidence Operating Systems" and "Computer-based Evidence - the Internet". A 'train the trainer' course is planned for January 2001. In addition, INTERPOL publishes two training manuals on the subject, which are disseminated to its 178 member nations. A training video is currently in production that will be disseminated to all INTERPOL members accompanied by a CD-Rom that will serve as an introduction on how to deal with computer-related crime and evidence. Here too, however, a lack of adequate resources prevents the Organization from keeping pace with this rapidly changing field of crime and from reaching a majority of its members. The governments of France and the U.K. are currently funding INTERPOL computer training initiatives in Africa.

As addressed in the response to Question No. 1, the collection of accurate statistical information on cyber crime cases is difficult at best. INTERPOL and its expert working parties should work to alleviate this problem by setting standards and definitions, and to bring, with the backing of the G8, legislative reality to these standards.

6. **Can you please discuss your working relationship with the private sector in your nation in cases where they are the victims of or unwitting participants in a cyber intrusion?**

   INTERPOL considers that it is vital to protect the global business infrastructure on which all economies depend. Recognizing that this infrastructure is at risk from high tech crime and taking into account the extraordinary rate of development of this type of crime and the "frontier-less" environment in which it takes place, it is essential that the public and private sectors work together in strategic alliance to challenge cyber criminals in the most effective ways possible. To that end, INTERPOL maintains sound relationships with a number of private sector concerns and businesses. It is currently exploring whether there may be viable possibilities for closer cooperation and information sharing with private sector firms. However, in order to avoid potential conflicts of interest and comply with all legal requirements on the data security, the preference is to work with the collective industry representatives and/or associations that are adversely affected by this type of crime (e.g., INTERPOL is currently in the process of completing an international training video in partnership with the Internet Alliance).

   The USNCB's involvement with the private sector is limited. The vast majority of USNCB cases originate directly from U.S. or foreign law enforcement component requests. Many of the requests concern private companies that become involved in some aspect of crime, and most of the cyber intrusion matters involve private corporations.

7. **Can you discuss current or proposed legislation in your nation for addressing cyber intrusions?**

   INTERPOL collaborates closely with a number of organizations, academic and other, involved in projects to collate and evaluate national legislation on computer crime. Their aim is to ultimately develop international standards and best practice measures in the area of cyber crime. One example of this is INTERPOL's work with the Council of Europe to develop a draft convention on cyber crime. Provisionally entitled "Draft Convention on Cyber-Crime", this Council of Europe text will be the first international treaty to address criminal law and procedural aspects of various types of offending behavior directed against computer systems, networks or data, as well as other similar abuses. This legally binding text aims to harmonize national legislation in the field, facilitate investigations and allow efficient levels of co-operation between the authorities of different States. The text should be finalized by a group of experts by December 2000 and the Committee of Ministers could adopt the text and open it for signature as early as Autumn 2001.

INTERPOL is currently finalizing a cooperative agreement with the G-8 Subgroup on High-Tech Crime, aimed at preventing duplication and the resulting waste of resources. It is hoped that this collaboration will result in the political backing for legislative changes to implement international standards and notification procedures through a single point-of-contact contact network.

8. **What means can you suggest for improving the process for obtaining evidence internationally--protected seizures, trans-border search and seizure, computer forensics, etc....?**

   The International Criminal Police Organization has established rules of police cooperation for its 178 Member countries. This framework facilitates and simplifies requests for criminal investigative assistance across borders, and works concurrently with ministerial arrangements for rendering mutual legal assistance.

   Given the proliferation of computer-related crimes and indications that this trend will continue, there is a recognized need to standardize methods of investigation, evidence collection, and forensic examination. Entities involved are making efforts to work within existing Mutual Legal Assistance Treaties and, when necessary, to identify areas where new legislation is required.

9. **What can you suggest to improve our capabilities to locate and identify criminals, and specifically the preservation of critical transactional data and other information that must be shared quickly?**

   The United States can leverage its membership in INTERPOL to help achieve improvement in the location, identification and rendering of criminals and fugitives. The INTERPOL network, connecting all 178 Member countries, is undergoing an upgrade that will permit state-of-the-art notification procedures and enable foreign law enforcement components, working in concert with private industry, to preserve transactional data and share critical information.

   Our ability to deal effectively and efficiently with cyber crime can be enhanced through continued coordination and cooperation among U.S. law enforcement agencies dealing with various aspects of cyber crime, and through competency building for less experienced enforcement agencies worldwide.

   INTERPOL maintains a secure website dedicated to sharing restricted law enforcement information on a variety of crime areas. It is currently working to establish secure access specifically for cyber crime investigators around the world, in order to enable the sharing of information, such as the Computer Crime Manual, in digital format.

10. Based on your own national experience, what can you suggest to other nations regarding governmental organization to detect, warn of, and respond to cyber intrusions?

As cyber crime is inherently international, the major focus should be on developing a broad contact network. However, one's national response in an international case is only as good as the ability and efficacy with which other international players respond. This point underlines the need for thorough competency building exercises and training programs to strengthen the weak links in the network and, in so doing, to develop effective regional responses.

INTERPOL membership and participation increases the likelihood of detection, timely notice and proper law enforcement response to cyber intrusions. It also permits access to a 24-hour network of national experts in approximately 40 countries, in a secure and confidential manner.

The International Criminal Police Organization
ICPO - Interpol

Aims

According to the terms of Article 2 of its Constitution, Interpol's aims are:

- To ensure and promote the widest possible mutual assistance between all criminal police authorities, within the limits of the laws existing in its member countries and in the spirit of the Declaration of Human Rights

- To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes

Article 3 of the Constitution adds:

- It is strictly forbidden for the Organization to undertake any intervention or activities of a political, military, religious or racial character.

Working principles

Interpol does not have teams of detectives with supranational powers who travel the world investigating cases in different countries. Briefly, international police co-operation is the co-ordinated action of the police services within Member States, all of which supply and request information and services.

As a mark of its determination to accomplish its mission with all due respect for individual rights and freedoms, Interpol has created an institution which is unique in international law: the Supervisory Board for the Control of Interpol Archives. This body ensures that information contained in Interpol databases is managed in strict accordance with the Organization's rules.

Areas of activity

Interpol's General Secretariat is the centre for co-ordinating the fight against international crime. Its activities, conducted at the request of police departments and judicial authorities in member countries or on its own initiative, are all focused on crime prevention and law enforcement in such sectors as:

> **Offences against persons and property** - including, for example, murder, kidnapping, hostage-taking, traffic in human beings, offences against minors, missing children, organised crime, terrorism, traffic in stolen motor vehicles, unlawful interference with civil aviation, firearms and explosives offences and disaster victim identification.
>
> **Offences involving cultural property** - such as art theft and trafficking and traffic in endangered species of wildlife.

Economic and financial crime - including currency and document counterfeiting and forgery, fraud of various types involving banking operations, commercial activity, investments, money laundering, traffic in radioactive substances and environmental crime.

Drug traffic and related offences - such as the illicit cultivation, manufacture, transport and sale of drugs.

International broadcasts and notices are circulated at the request of member countries about criminals who are wanted or liable to operate at international level, and about missing persons (children in particular), unidentified bodies, stolen property and methods used by criminals.

Liaison and co-ordination activities are conducted in connection with investigations. Regional structures have been established to strengthen international police co-operation. Criminal intelligence is analysed centrally and shared with member countries where this is beneficial.

Deliberative institutions

The General Assembly is composed of delegates from member countries. It meets once a year to take all the major decisions concerning the Organization's future. The Executive Committee has thirteen members (including the President of the Organisation). The Committee ensures that General Assembly decisions are implemented and also prepares certain topics for discussion by the Assembly.

Permanent structures for co-operation

The General Secretariat is administered by the Secretary General who is appointed by the General Assembly. The Secretariat implements the decisions taken by the General Assembly and the Executive Committee and is responsible for running the day-to-day business of international co-operation from the Organisation's General Secretariat.

Each Member State provides a National Central Bureau (NCB). This is the national department which serves as the permanent focal point for international police co-operation. An NCB liaises with other authorities in its own country, the other NCBs and with the General Secretariat, and has direct access to Interpol's rapid and secure telecommunications network and databases.

Resources

The General Secretariat is administered by the Secretary General who is appointed by the General Assembly. The Secretariat of some 360 staff, from about sixty countries, includes police officers, analysts, technicians and administrators. It implements the decisions taken by the General Assembly and the Executive Committee, and maintains the day-to-day business of international police co-operation.

The Organization's budget (just $32 million in 1999) is mainly financed by contributions from Member States. Interpol's four official languages are Arabic, English, French and Spanish.

Interpol history

1914	First International Criminal Police Congress in Monaco: the establishment of an **international criminal records office** and the harmonisation of extradition procedures proposed.
1923	Second International Criminal Police Congress in Vienna: the **International Criminal Police Commission** (ICPC) was established, with its Headquarters in Vienna.
1946	Revival of the ICPC after the Second World War: Paris became the Headquarters, new Statutes were adopted and the word **'Interpol'** was used for the first time
1956	The ICPC became the International Criminal Police Organisation (ICPO-Interpol)
1984	A new Headquarters Agreement with France came into force; the General Assembly adopted resolutions on countering terrorism.
1989	Following its transfer from St Cloud, near Paris, where it had been located since 1966, the Organisation's new General Secretariat building in Lyons (France) was officially inaugurated on 27th November
1997	The ICPO-Interpol had 177 member countries (50 in 1955, 100 in 1967)

Mr. HORN. Thank you very much. That is a very helpful statement. We now move to Mr. Richard Schaeffer, Jr., Director, Infrastructure and Information Assurance, Office of the Assistant Secretary of Defense for Command Control Communication and Intelligence. Join us up here, and we will join the others also. If we might get you all around that table, we would appreciate it, if the staff would do that. Might get another table over here. But we like to have a dialog once we are done with all of the presenters, and I would just as soon have everybody at the same table if that is possible.

Mr. Schaeffer, please proceed.

STATEMENTS OF RICHARD C. SCHAEFFER, JR., DIRECTOR, INFRASTRUCTURE AND INFORMATION ASSURANCE, OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATION, AND INTELLIGENCE); MARIO BALAKGIE, CHIEF INFORMATION ASSURANCE OFFICER, DEFENSE INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE; AND JACK BROCK, DIRECTOR, GOVERNMENTWIDE AND DEFENSE INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE

Mr. SCHAEFFER. Thank you, Mr. Chairman. I appreciate the opportunity to be here today to discuss this very important topic.

To set the stage for my remarks, I'd like to say a few words about the environment in which the Department of Defense [DOD], conducts its daily operations during peacetime, during crisis, and even during war.

The Department's steadily increasing dependence on a global information environment over which it has little control heightens its exposure and vulnerability to a growing number of increasingly sophisticated internal and external threats. Globally internetworked and interdependent information systems tend to level the playing field between allies and adversaries and offer adversaries access to potentially high value, low risk information infrastructure targets.

These targets, if successfully attacked, have the potential to impact the full spectrum of DOD operations. To attack a large number of systems, an adversary need only find and attack a single exploitable connection to the system. Once inside the system, an adversary can exploit it and the systems networked to it. Further, with every advance in information technology, new vulnerabilities are created that must be quickly discovered and effectively neutralized.

Providing for the protection of the defense information infrastructure is one of the Department's highest priorities and most formidable challenges. Within the DOD, we have established detailed procedures for the coordination of all cyber events. The Joint Task Force-Computer Network Defense [JTF–CND], was formed on December 30, 1998, to provide a single command with the authority to coordinate and direct the defense of the DOD computer systems and networks.

Prior to the formation of the JTF, no single entity had the authority to coordinate and direct a DOD-wide response to a computer network attack. The JTF-CND and the NIPC, the National

Infrasfructure Protection Center, form a strong collaborative team for dealing with attacks on DOD systems.

Over the past 18 months, the JTF-CND has developed processes for identifying attacks against DOD networks, assessing the importance of those attacks, notifying appropriate headquarters of the information, developing and implementing responses to them, and coordinating with external organizations such as the NIPC. The DOD relies on the NIPC to coordinate cyber attack indications and warning with the Nation's critical infrastructure elements—communications, power, etc.—upon which the Department depends for mission success.

In closing, I would like to say a few words about where we are today and where we need to be in the future. Today it takes us at best hours to transition from detection to warning. At worst this could be days. The attacks are perpetrated and executed in milliseconds. We must develop the technology, capabilities, processes, and legal framework to respond to cyber events in real-time. There will come a time when our capabilities will be tested, and national security or the economic security of the Nation will depend on components like the JTF-CND, NIPC and others working collaboratively in response to the event.

I want to thank the subcommittee again for providing an opportunity for the Department of Defense to present its views on this very important issue, and we look forward to continuing to work with Congress to ensure that we are able to meet these ever increasing challenges.

[The prepared statement of Mr. Schaeffer follows:]

Statement for the Record

Mr. Richard C. Schaeffer Jr.
Director, Infrastructure and Information Assurance
Office of the Assistant Secretary of Defense
(Command, Control, Communication, and Intelligence)

before the

Subcommittee on Government Management, Information, and Technology

On the challenges of providing a coordinated response to computer security threats.

July 26, 2000

Introduction:

Mr. Chairman, and Members of the Committee, I appreciate the opportunity to be here today to discuss this very important topic in relation to the challenge of providing a coordinated response to computer security threats.

To set the stage for my remarks I'd like to say a few words about the environment in which the Department of Defense (DoD) conducts its daily operations—during peacetime, crisis, and war. The Department's steadily increasing dependence on a global information environment, over which it has little control, heightens its exposure and vulnerability to a rapidly growing number of increasingly sophisticated internal and external threats. Globally internetworked and interdependent information systems tend to *level the playing field* between allies and adversaries, and offer adversaries access to potentially high-value and (currently) low-risk information infrastructure targets. These targets, if successfully attacked, have the potential to impact the full spectrum of DoD operations. To attack a large number of systems, an adversary need only find and attack a single exploitable connection to the system (through the use of a wide and growing variety of commonly available and inexpensive hacker tools). Once inside a system, an adversary can exploit it and the systems networked to it. This global marriage of systems and networks creates what has become a *shared risk environment.* Further, with every advance in information technology, new vulnerabilities are created that must quickly be discovered and effectively neutralized.

Given the risks and the fact that weakness in any portion of the Defense Information Infrastructure (DII) is a threat to the operational readiness of all Components, the Department is moving aggressively to ensure the continuous availability, integrity, authentication, confidentiality, and non-repudiation of its information and the protection of its information infrastructure. Exercises and real-life events clearly demonstrate that Defense-wide improvement in Information Assurance (IA) is an absolute and continuous operational necessity. We can no longer be satisfied with reactive or after-the-fact solutions. As the Department modernizes its information infrastructure, it must also continuously invest in the research, development, and timely integration of products, procedures, and training necessary to sustain its ability to defend it. Providing for the protection of the DII is one of the Department's highest priorities and most formidable challenges.

However, *perfect* protection is an unattainable goal. As stated above, an adversary need only find and attack a single exploitable connection to the system. This location could be at any base, post, camp or station, worldwide. It could be the location of an elite military unit or an entirely civilian element responsible for the extraordinary range of support activities critical to the successful execution of DoD missions.

The first challenge we face is to identify that an *attack* has occurred. I use the term *attack* here in a very broad sense to mean any malicious event perpetrated by an unauthorized (or authorized) user of a DoD information system. This is a non-trivial problem. Yes, there is technology available today to detect anomalous events. And, while this technology continues to increase in capability, for the most part, it will always lag behind the capability of the adversary, particularly the sophisticated adversary, to develop new attack capabilities. Within the Department, we have deployed a vast array of sensors to provide indications and warning of an ongoing attack. Once anomalous activity is detected the process of sorting through vast amounts of audit data is then required to attribute the attack to a specific person, organization, or entity (to include nations states and/or transnational elements). As a point of reference, during 1999, over 22,000 *attacks* were reported to the Joint Task Force-Computer Network Defense (JTF-CND).

The next challenge is *attribution.* Within U.S. borders, any attack is viewed first as a law enforcement (LE) issue—it's viewed as a *crime* rather than a national security matter. If, and only if, it can be shown that the attack is being perpetrated by a foreign entity, from foreign soil, does the attack become a national security matter. Because of the anonymity with which attacks can be perpetrated, and the ease with which an attacker can move from one computer (Host) to another, the delay in identifying the adversary, let alone their intention(s), can be very long.

Attribution is a complex undertaking that requires coordination among several elements. [In this context, a host is any computer from which an attack is launched. This could be an attacker's own computer, a server at a local Internet Service Provider (ISP), a server at a U.S. college or university, or a server at another government department or agency.] Under our constitutional system, information essential to *attribute* the attack to a specific entity typically can be gathered only pursuant to criminal investigative authorities. The host owner can, or course, cooperate with law enforcement officials without the need for a warrant, and fortunately this frequently occurs. Regardless, collection and analysis of audit data from the host is a necessary component of the attribution process. A court order must be obtained, which can take from hours to days, and then the data must be obtained and analyzed. I don't want to over simplify the analysis process—it is extremely difficult. It is this analysis, together with other information gained as part of the investigative process (and, as appropriate, intelligence processes) that provides a picture of the perpetrator's, motivation, and purpose. Coordination between responsible elements, both internal and external to the DoD during these activities is essential.

Within the DoD, we have established detailed procedures for the coordination of all cyber events. The JTF-CND was formed on December 30, 1998 to provide a single command with authority to coordinate and direct the defense of the DoD computer systems and networks. Originally formed as a separate JTF reporting directly to the Secretary of Defense, JTF-CND became a direct reporting command of U.S. SPACE Command on October 1, 1999 when SPACE Command was assigned the mission of computer network defense for the Department of Defense. The JTF-CND provides DoD with a focal point for dealing with cyber threats and answered the "Who's in charge?" question. Prior to the formation of the JTF, no single entity had the authority to coordinate and direct a DoD wide response to a computer network attack. The JTF-CND and the National Infrastructure Protection Center (NIPC), which serves as a focal point for the Federal Government's efforts to detect, assess, warn of, and respond to cyber attacks, form a strong collaborative team for dealing with *attacks* on DoD systems and networks.

Several examples are provided to elaborate on the responsibilities of the JTF-CND.

> During the Melissa Virus incident in March 1999, the JTF-CND, in cooperation with the DoD Computer Emergency Response Team (CERT) and the JTF's Service components, was able to quickly assess the threat, develop a defensive strategy, and direct appropriate defensive actions. Despite damage to the private sector in the hundreds of millions of dollars, DoD experienced relatively little effect and no operational impact.
>
> The JTF-CND began working on countermeasures for distributed denial of service tools in November 1999. While not finding any direct antidote, the efforts provided significant data for the creation of a DoD functional plan for countering this type of attack while simultaneously ensuring that DoD systems are not subverted into taking part in attacks on others.
>
> The JTF was at the center of DoD's response to the Year 2000 event. The JTF provided valuable staff analysis of the situation, and coordinated with the numerous ad hoc organizations formed to implement the federal government's response. The JTF was integral in ensuring that DoD took a coordinated and measured approach.
>
> The ILOVEYOU virus provided another example of rapid action. The JTF staff rapidly identified the potential damage and provided rapid notification to the CINCs, Services and agencies that enabled them to effectively respond.

Over the last 18 months, the JTF-CND has developed processes for identifying attacks against DoD networks, assessing the importance of those attacks, notifying appropriate headquarters of the information, developing and implementing responses to them, and coordinating with external organizations such as the NIPC. The DoD relies on the NIPC to coordinate cyber attack indication and warnings with the nation's Critical Infrastructure elements (Communications, Power, etc.) upon which the Department depends for mission success.

In closing, I'd like to say just a few words about where we are today and where we need to be in the future. Today it takes us, at best, hours to transition from detection to warning; at worst this could be days—the attacks are executed in milliseconds. We must develop the technology, capabilities, processes, and legal framework to respond to cyber events in near real time. There will come a time when our capabilities *WILL* be tested and national security or the economic security of the nation will depend on components like the JTF-CND, NIPC, and others working collaboratively in response to the event.

I want to thank the subcommittee again for providing an opportunity for the Department of Defense to present its views on this very important issue. I look forward to working with Congress to ensure that we are able to meet these ever increasing challenges.

Mr. HORN. Thank you very much. That is a helpful statement, and I am delighted to see that they have got some depth over there under that Assistant Secretary, because we worried through Y2K after the general retired.

So we now go to Mario Balakgie, Chief Information Assurance Officer, Defense Intelligence Agency, Department of Defense.

Mr. BALAKGIE. Thank you, Mr. Chairman and members of the committee. I am honored to be here to have this opportunity to speak on the challenge of coordinating response to computer security threats. I am here to present the views and opinions of the Defense Intelligence Agency within our role for information assurance mission of the Defense Intelligence Community.

The business of intelligence is unique because of what we do. But when it comes to how we operate, we are driven by the information age. We rely on a global information infrastructure using technology as an integral tool to carry forward our mission of intelligence. Unlike in the past we now operate in an interconnected and interdependent environment, giving us tremendous benefit but not without security risk to our information infrastructure.

Today's challenge is to ensure the protection of those infrastructures against the cyber threat and requiring a community-wide approach to a coordinated and active defense. Whether it is the Intelligence Community, the larger Federal Government or the private industry, each face common impediments to conducting a coordinated response.

The interconnected environment has opportunities and risks. The worldwide nature of threats, the attacks from anyone at any time, does not discern organizational boundaries. The reality of threat presents fundamental challenges and they are: our ability to detect the cyber event through the use of real-time sensors; discerning if the event is an attack or an anomaly; conducting timely analysis to determine attribution and finally reacting.

To further complicate a coordinated response there are existing varying protection policies within interconnected communities, making it difficult to execute an all encompassing defensive action. For example, the various owners of networked infrastructures do not necessarily agree on what may or may not be constituted as an attack, how to respond to a cyber attack or what defensive measures are required.

The most significant issue we face in conducting coordinated response of cyber threat is the demands for skilled and qualified personnel who have an understanding of information and security technologies. In particular, intrusion detection systems require specialized skills to monitor networks for incident detection, conduct analysis of anomalies and ultimately react.

While we can implement sophisticated security technology, without these trained professionals, even our best security defenses will not be effective.

The Defense Intelligence Community has several initiatives under way to ensure our incident response and defensive efforts are coordinated. Those initiatives are described in my statement, but I would like to point or highlight at least one of them, and that is risk management.

For us to understand our infrastructure strengths and weaknesses, we are integrating risk management as a business practice to determine critical assets, protection requirements, and establishing priorities. Risk management will enable us to emphasize the business process whereby resource decisions are made in a consistent and methodical manner.

Finally, our response to cyber threats shouldn't be misconstrued as a one-time issue but rather a never ending challenge. We must commit to the information assurance mission constant vigilance and protecting the information infrastructure. Our defensive efforts must be comprehensive in nature and include coordinated strategies within the government as well as private industry.

This challenge is best characterized as a long-term business of risk management balanced against threats, vulnerabilities and ultimately the return of our investment. On behalf of the Defense Intelligence Agency, thank you for the opportunity to present our views and opinions.

[The prepared statement of Mr. Balakgie follows:]

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

Committee on Government Reform

TESTIMONY
of

Mario Balakgie
Chief Information Assurance Officer
Defense Intelligence Agency

before a hearing
of the

Subcommittee on Government Management,
Information, and Technology

July 26, 2000

"Challenges of Coordinated Response to Computer Security Threats"

Opening

Thank you, Mr. Chairman and members of the Subcommittee. I am honored to be here and pleased to have this opportunity to speak on the issue of cyber threat and response.

I am the Chief Information Assurance Officer for the Defense Intelligence Agency (DIA). I manage the Information Assurance Program of the Defense Military Intelligence Community, a function of our Agency's Chief Information Officer. I have been involved with this program for approximately eight years and have gained practical insight regarding the cyber security response in the new world of the Information Age. I will be presenting what DIA views as issues and challenges for information assurance of our global information infrastructure.

The Defense Military Intelligence Community is comprised of the intelligence organizations within the Services and Commands. These organizations are global in mission and interact as a single community in which DIA has lead role for military intelligence production. This community is also a member of the National Intelligence Community.

Role of Information Technology

Defense intelligence uses information technology as an integral tool to perform our intelligence mission of collection, analysis, production, and dissemination. We operate in a globally interconnected and interdependent series of networks with high-speed links providing real time data, video, and voice capabilities. This network infrastructure is secured from end to end and transmits sensitive intelligence information to our senior decision-makers, operational forces, and affiliates. The employment of Information Technology has been a key enabler to our success and has provided a tremendous return of our investment but, not without taking on a proportional risk to the security of our information infrastructure.

Because of our intelligence mission and the inherent sensitivity of our work, we were at one time protected simply through maintaining network isolation and separation from the rest of the world and sometimes even within our own Intelligence Community. Such an isolated mode of operation completely changed with the introduction and subsequent invasion of networked computers at virtually every level of our intelligence business. The new interdependent environment has brought about both opportunities and risks to our information infrastructure. This means our response to computer threats is now very different from the traditional approach given that a single attack can potentially affect an entire information infrastructure. Today's technological dimension not only requires a coordinated response but also necessitates active defense, meaning offensive actions must taken to preempt cyber attacks.

Information Assurance

Information Assurance is the function of protecting and defending information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. More than ever before our Information Assurance business is essential as we contend with unsurpassed challenges (threats as well as opportunities) to our information infrastructure.

Given the risks and the fact that weakness in any portion of our network is a threat to the operational readiness of all connections, our Information Assurance goal is to ensure the continuous availability of our systems and networks. The technical strategy that underlies our Information Assurance program is Defense-in-Depth in which layers of defense are used to achieve balanced, overall protection. Defense-in-Depth maximizes our ability to protect information and defend our network infrastructure through the implementation of layers of security solutions. The security layers are a combination of technical (hardware and software) capability, policy, and operations. Our overall strategy for Information Assurance is to achieve enterprise-wide infrastructure protection, with our defense layers guaranteeing delivery of accurate, reliable, and timely information.

Opportunities and Threats

The last several world crises demonstrated our extraordinary reliance on the information infrastructure. Defense intelligence relies on global networks to support deployed forces involved in current crises, as well as pre- and post-operations. In providing vital information to the warfighting units, the information network has become a combat power. However, our reliance on the network and system strength can become a point of vulnerability. Consistent and well-defined Information Assurance objectives are key to defending the network infrastructure and ensuring our ability to successfully conduct military operations.

We are challenged because the environment is constantly changing as a result of threats. System and network vulnerabilities are continuously discovered on the Internet and these same vulnerabilities can be used to exploit our information networks. Although intelligence systems operate in a secure environment, they are comprised primarily of the same commercial-of-the-shelf products used in unclassified environments, and are subject to the same vulnerabilities.

Another significant threat area is that of the insider. An insider is anyone who currently has, or has in the past, been authorized access to a government information system. These can be military members, federal employees, or employees of the private sector. In a recent example, an investigation concluded that the insider threat accounted for 87% of identified intrusions into Department of Defense information systems. This is truly alarming. It is a concern for all government organizations and it requires immediate preventive actions for mitigating the threat. These measures include strengthening personnel security, detection and response to problems, and protecting information assets.

There are a number of information assurance activities that will continue to be challenging in the dynamic world of technology and cyber security response. By concentrating on a few basic tactics we can, however, make progress in implementing effective short-term proactive measures to protect the infrastructure. These priority security measures address the immediate threats we face today. The Defense Intelligence Community is concentrating its resources on five defensive areas in part of our efforts to institute a comprehensive and effective coordinated defense.

- Risk Management as a Business Process: A critical factor is our ability to identify and mitigate risks to our information infrastructure. Herein lies the role of risk management for aiding us in understanding infrastructure vulnerabilities and making important decisions as to what is or is not an acceptable security posture. Risk management is integral to the information technology cycle and must be incorporated as a business process.
- People Focus: The most important element of our Information Assurance program is the human factor. Personnel -- both users and information technology professionals -- are the first line and most important defense. Information Assurance professionals responsible for security management must be trained and certified with a prerequisite level of skills and competencies. While we can implement sophisticated security technology, without trained professionals who understand the technology, even our best security defenses will not be effective.
- Mitigate Insider Threat: Minimizing the potential damage by an insider requires specific strategies that are part of an active security program. This includes identifying critical information, establishing trustworthiness,

strengthening personnel security, detecting insiders, and taking corrective action.

- Implement Intrusion Detection Systems: Implementing intrusion detection systems provides attack sensing and preempting serious incidents. However, intrusion detection technology has not yet advanced to the stage of detecting and responding to a sophisticated, organized attack[er]. Additionally, there are challenges in supporting the operations of intrusion detection systems since they require a skilled individual who can quickly and accurately distinguish an anomaly from an attack.
- Vulnerabilities and Exploits Awareness: We are faced daily with new vulnerabilities to our systems and networks. Many of these vulnerabilities are exceptionally dangerous and cause significant concern. To further challenge us many of these exploits are publicly discovered and globally distributed via the Internet. Our response is to diligently be aware of vulnerabilities via public and private security advisories and take offensive action to mitigate potential exploits.

Response Challenges

Technology has brought us to the point where global interconnections of the information infrastructure are a permanent and irreversible business aspect. This reality incorporates threats for all infrastructures. Hence the realization of shared risk. Effectively addressing the threats and vulnerabilities to systems and networks requires a constant level of sensitivity and awareness to computer attacks, exploitation techniques, and coordinated response.

There are several obstacles in coordinating a response. These include conflicting protection policies as well as authorities of the information infrastructure. At the least, this makes execution of defensive actions difficult. The "worldwide" nature of threats -- attacks from anywhere at anytime -- is also a reality. Not only are these attacks difficult to detect but, more importantly, they present an attribution problem when sophisticated attackers are involved. Additionally, our reliance on commercial-off-the-shelf products places our infrastructure at risk because much of the vendor software contains publicly known [exploits] that are then used against us. Finally, the interconnected world that provides valuable information sharing capabilities also presents the means for conducting large-scale attacks with tremendous speed.

Improving coordinated responses between the private and public sectors is essential since both are stakeholders of the national, critical infrastructures. These are the same infrastructures that are vulnerable to the same threats mutually faced by all today. To succeed in protecting our information networks, both the private and public sectors must work together and coordinate efforts in planning and responding to the constant challenge of information protection.

Recognizing the need for coordinated response, the Department of Defense has stepped out aggressively to address a global, computer network defense. The United

States Space Command and its Joint Task Force for Computer Network Defense (JTF-CND) was established with the primary mission for coordinating such responses. JTF-CND's mission is to coordinate and direct the defense of Department of Defense computer systems and networks. This includes the coordination of defensive actions with non-Department of Defense government agencies and appropriate private organizations.

Summary

Response to computer security threats is indeed a challenge and should not be misconstrued as a one-time issue. Hence, we must commit to the information assurance mission with constant vigilance in protecting the information infrastructure. This demands skilled people and crucial security technology for defending our global systems and networks. For maximum results our defensive efforts must be comprehensive in nature and include coordinated strategies between the private and public sectors.

The business of information infrastructure protection is a never-ending journey. We have attained several goals for improving our ability to defend the network but there is much that remains to be achieved. The challenge is continuous, incorporating the dynamics of technology and the global magnitude of the infrastructure. This perpetual challenge is best characterized as a business of risk management balanced against threats, vulnerabilities, and ultimately the return of our investment.

Mr. HORN. I am going to take the chairman's right to ask a question at this point. I would be curious as to the biometrics—I am very interested in your insider bit because that is what often does and has a real problem in either the private sector, the public sector, whatever, to what degree are we moving fairly rapidly to that so we would be able to at least deal with where the insider is and either to lock him out or lock him in?

Mr. BALAKGIE. Well, the first challenge for us is to detect the insider and we are relying on the use of intrusion detection systems to be able to do that. Those technologies are currently implemented with a variety of sensors, what we refer to as sensors, throughout our infrastructure.

They are—the sensors are gauged, if you will, to detect certain events. Those events trigger a warning and then we in turn pursue what could be an insider.

I would tell you that the technology is mature; however, against a sophisticated insider, this still presents a challenge in determining who they are and what they're doing.

Mr. HORN. Well, thank you very much. I am sure my colleagues will have questions later. Our next presenter is Mr. Jack Brock, well-known to this subcommittee. He is the Director of Governmentwide and Defense Information Systems for the U.S. General Accounting Office, an arm of the legislative branch. Mr. Brock.

Mr. BROCK. Thank you very much, Mr. Horn. It is always a pleasure to be here. I feel like I am at my grandmother's dining room at Christmas time. It is good to have a seat at the table. It is crowded.

Mr. HORN. I apologize that we did not think about it to start with.

Mr. BROCK. I think you heard from most of the witnesses that we live in a world where we are talking about a cyber threat that is not defined by geographic boundaries, and the lack of traditional boundaries really presents a challenge to nations to consider new strategies and new ways of dealing with this. No longer are you dealing in a physical world where you can more easily recognize the threat, but where you frequently have more time to react to the threat. The threat is there. It is sudden, it is real, and you have to react immediately.

Further, the ownership of the problem is not just with the national governments. It resides with all elements of the critical infrastructure. And that can be public utilities, it could be the financial sector, as well as Federal agencies, but a whole variety of players are involved here and they all need to be at the table. I think today you got a good overview from the law enforcement agencies, but if you had a different panel tomorrow and you had people from the financial sector or people from the telecommunications, you might be getting a slightly different perspective. The problem might be the same, but the response and the reaction to it could well be different.

Further, this infrastructure that these organizations deal in is complicated by the exponential spread and support evolution of information technology. And frequently the technology and the ability to exploit that technology runs ahead of the ability to detect and respond, and that is a very serious problem.

There are three elements to this issue. First, do we need to be concerned about it? Second, if we do need to be concerned about it, what are the challenges that have to be overcome to have an effective response? And then, third, how do we begin to address the challenges?

First on the threat, I don't need to repeat what these gentlemen have all told you. There is a very real threat and that threat can come from an insider. That threat can come from a lone hacker who is out for a joy ride, from an organized group of hackers, from a terrorist group or, as NSA estimates, from 1 of over 100 countries that now have the capability of launching an offensive cyber attack.

I think the potential for real damage has been highlighted by the "ILOVEYOU" virus, the denial of service, the Melissa virus. While none of these caused catastrophic damage in an overall sense, it demonstrated the very real potential for damage by cyber attack.

The challenges, we have identified in the statement four challenges. First of all, establishing trust relations. You have so many people that are at the table, just like we are at this table, that have to work with one another. And even though law enforcement people might work together, share information, frequently the private sector do not want to share information with the law enforcement. They see it as a one-way street. You give information but you don't get anything back.

You have to establish a trust relationship between different government entities, some who have less than friendly relationships with each other. You have to establish relationships between the government and the private sector. You have to balance off national security versus economic threat. There are a whole series of relationships that have to be established, and it is really not realistic to assume that everyone shares the same perspective or views the threat in the same way or views the response in the same way.

The second challenge is related to that, but it goes to reporting needs and mechanisms. What kind of information do you need to be responsive? How do you best share it? What's the protocol for sharing it and how do you do it in a timely manner so that it is effective?

Third, and this was touched upon by several panel members, are the need for technical capabilities. We have a real lack of technical skills within the government, and I think elsewhere, for dealing with this. Computer security is clearly underfunded and underrepresented in most agencies. Most agencies or many agencies do not have the skills that are necessary to provide a level of protection.

We lack intrusion monitoring systems. The Department of Defense has taken a real leadership role in moving out on this, but this is still a very new area where we don't have the systems in place that can effectively monitor intrusions.

And last, and I think the thing that bothers us the most right now is what the national plan calls for in making the Federal Government a model. And as you know from prior statements before you, the Federal Government is far, far away from being a model. Virtually every Federal agency has severe computer security problems that put their operations at risk. And if the Federal Government is going to be in a position to speak about the need for developing national and international infrastructures, it needs to get its own house in order and we are far from that.

In terms of addressing the challenge, as you heard today, a lot is being done. There are a lot of organizations that are sharing information. These organizations certainly exist within the United States and they certainly exist internationally. But within our own government, that's done without an effective framework. The national plan for information systems protection, which the first version was issued earlier this year, lays out the beginning of a framework dealing with Federal Government. The next version is supposed to bring in the international and private sector, but a framework is a long ways away from having an effective implementation of the policies that are needed to in fact do the balancing act that you need between the various sectors to establish the trust relationships, to develop the effective coordination mechanisms that are required to address the challenge.

So the challenges to be addressed is a comprehensive framework. This needs to be developed, it needs to be vetted, it needs to be bought into. It needs to allow each of the components to clearly define their individual needs. There needs to be an opportunity to balance these needs against the national need and, last, to develop and implement strategies to meet those needs.

This is going to take leadership. This is going to take a real commitment, a prolonged commitment, it will take time and undoubtedly take a great deal of money.

That concludes my summary, Mr. Chairman.

[The prepared statement of Mr. Brock follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Wednesday
July 26, 2000

CRITICAL INFRASTRUCTURE PROTECTION

Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination

Statement of Jack L. Brock, Jr.
Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

GAO
Accountability * Integrity * Reliability

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the challenges of providing a coordinated response to computer security threats. As you know, computer security risks have increased dramatically over the last decade as our government and our nation have become ever more reliant on interconnected computer systems to support critical operations and infrastructures, including telecommunications, finance, power distribution, emergency services, law enforcement, national defense, and other government services. These interconnected systems are part of a global information infrastructure that is not defined by geographic boundaries or by unity of purpose among the individual components of the infrastructure. To a large extent, these components are developed and maintained by private companies and, in some cases, foreign entities. This situation is challenging nations to consider new strategies for protecting sensitive data and information-based assets, in part through information sharing and coordination between public and private organizations--sometimes on an international scale.

Today, I would like to discuss the challenges to achieving effective coordination that we have identified over the last 2 years. Such challenges--which include establishing trust relationships between the government and private sector, developing the mechanisms of gathering and sharing data, strengthening technical capabilities, and providing stronger governmentwide leadership and continuity for critical infrastructure protection--

need to be successfully addressed in order to institute effective information sharing and coordination mechanisms among individual components of the infrastructure.

INCREASING NEED FOR COORDINATED RESPONSE

Since the early 1990s, the unprecedented growth in computer interconnectivity, most notably growth in use of the Internet, has revolutionized the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous in terms of facilitating communications, business processes, and access to information. However, without proper safeguards, this widespread interconnectivity poses enormous risks to our computer systems and, more importantly, to the critical operations and infrastructures they support.

While attacks to date have not caused widespread or devastating disruptions, the potential for more catastrophic damage is significant. Official estimates show that over 100 countries already have or are developing computer attack capabilities. Hostile nations or terrorists could use cyber-based tools and techniques to disrupt military operations, communications networks, and other information systems or networks. The National Security Agency has determined that potential adversaries are developing a body of knowledge about U.S. systems and about methods to attack these systems. According to Defense officials, these methods, which include sophisticated computer viruses and automated attack routines, allow adversaries to launch untraceable attacks from anywhere in the world. According to a leading security software designer, viruses in particular are becoming more disruptive for computer users. In 1993 only about 10 percent of known viruses were considered destructive, harming files and hard drives. But now about 35 percent are regarded as harmful.

Information sharing and coordination among organizations are central to producing comprehensive and practical approaches and solutions to these threats.

- First, having information on threats and on actual incidents experienced by others can help an organization better understand the risks it faces and determine what preventative measures should be implemented.
- Second, more urgent, real-time warnings can help an organization take immediate steps to mitigate an imminent attack.
- Lastly, information sharing and coordination are important after an attack has occurred to facilitate criminal investigations, which may cross jurisdictional boundaries. Such after-the-fact coordination could also be useful in recovering from a devastating attack, should such an attack ever occur.

The recent episode of the ILOVEYOU computer virus in May 2000, which affected governments, corporations, media outlets, and other institutions worldwide, highlighted the need for greater information sharing and coordination. Because information sharing mechanisms were not able to provide timely enough warnings against the impending attack, many entities were caught off guard and forced to take their networks off-line for hours. Getting the word out within some federal agencies themselves also proved difficult. At the Department of Defense, for example, the lack of teleconferencing capability slowed the response effort because Defense components had to be called individually. The National Aeronautics and Space Administration (NASA) had difficulty communicating warnings when e-mail services disappeared, and while backup communication mechanisms are in place, NASA officials told us that they are rarely tested. We also found that the few federal components that either discovered or were alerted to the virus early did not effectively warn others. For example, officials at the Department of the Treasury told us that the U.S. Customs Service received an Air Force Computer Emergency Response Team (AFCERT) advisory early in the morning of May 4, but that Customs did not share this information with other Treasury bureaus.

Current Information Sharing and Coordination Efforts

The federal government recognized several years ago that addressing computer-based risks to our nation's critical infrastructures required coordination and cooperation across federal agencies and among public- and private-sector entities and other nations. In May 1998, following a report by the President's Commission on Critical Infrastructure Protection that described the potential devastating implications of poor information security from a national perspective, the government issued Presidential Decision Directive (PDD) 63. Among other things, this directive tasked federal agencies with developing critical infrastructure protection plans and establishing related links with private industry sectors. It also required that certain executive branch agencies assess the cyber vulnerabilities of the nation's critical infrastructures—information and communications; energy; banking and finance; transportation; water supply; emergency services; law enforcement; and public health, as well as those authorities responsible for continuity of federal, state, and local governments.

A variety of activities have been undertaken in response to PDD 63, including development and review of individual agency critical infrastructure protection plans, identification and evaluation of information security standards and best practices, and efforts to build communication links. In January 2000 the White House released its *National Plan for Information Systems Protection*[1] as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future.attacks. The plan focuses largely on federal efforts being undertaken to protect the nation's critical cyber-based infrastructure. Subsequent versions are to address protecting other elements of the nation's infrastructure, including those pertaining to the physical infrastructure and specific roles and responsibilities of state and local governments and the private sector.

Moreover, a number of government and private sector organizations have already been established to facilitate information sharing and coordination. These range from groups that disseminate information on immediate threats and vulnerabilities, to those that seek to facilitate public-private sector information sharing on threats pertaining to individual infrastructure sectors, and those that promote coordination on an international scale.

[1] *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue,* The White House, January 7, 2000.

At the federal level, for example, the National Infrastructure Protection Center (NIPC), located at the Federal Bureau of Investigation (FBI), is to serve as a focal point in the federal government for gathering information on threats as well as facilitating and coordinating the federal government's response to incidents impacting key infrastructures. It is also charged with issuing attack warnings to private sector and government entities as well as alerts to increases in threat conditions. The Federal Computer Incident Response Capability (FedCIRC) is a collaborative partnership of computer security and law enforcement professionals established to handle computer security incidents and to provide both proactive and reactive security services for the federal government. In addition, the National Institute of Standards and Technology (NIST) is working to facilitate information sharing in the security community by building a database containing detailed information on computer attacks and the Critical Infrastructure Assurance Office (CIAO) is working to coordinate private sector participation in information gathering in the area of cyber assurance. The Administration is also undertaking efforts to facilitate information sharing with other nations.

Examples of other organizations focusing on information sharing and coordination include the following:

- Carnegie Mellon University's CERT Coordination Center,[2] which is charged with establishing a capability to quickly and effectively coordinate communication among

[2] Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency.

experts in order to limit damage, respond to incidents, build awareness of security issues across the Internet community.

- The System Administration, Networking, and Security (SANS) Institute, which is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions for challenges they face.
- The National Coordinating Center for Telecommunications, which is a joint industry/government organization that is focusing on facilitating information sharing between the telecommunications industry and government.
- The Financial Services Information Sharing and Analysis Center, which is a similar organization that exclusively serves the banking, securities, and insurance industries.
- Agora, which is a forum that is composed more than 300 people from approximately 100 companies and 45 government agencies, including Microsoft, Blue Shield, the FBI, U.S. Secret Service, U.S. Customs Service agents, and the Royal Canadian Mounted Police as well as local police, county prosecutors, and computer professionals from the Pacific Northwest. Members voluntarily share information on common computer security problems, best practices to counter them, protecting electronic infrastructures, and educational opportunities.
- The Forum of Incident Response and Security Teams (FIRST), which provides a closed forum for incident response and security teams from 19 countries to share experiences, exchange information related to incidents, and promote preventative activities.

- The International Organization on Computer Evidence, which provides an international forum for law enforcement agencies to exchange information concerning computer crime investigation and related forensic issues.

CHALLENGES TO EFFECTIVE COORDINATION

Developing the information sharing and coordination capabilities needed to effectively deal with computer threats and actual incidents is complex and challenging but essential. Data on possible threats--ranging from viruses, to hoaxes, to random threats, to news events, and computer intrusions--must be continually collected and analyzed from a wide spectrum of globally distributed sources. Moreover, once an imminent threat is identified, appropriate warnings and response actions must be effectively coordinated among government agencies, the private sector, and, when appropriate, other nations. It is important that this function be carried out as effectively, efficiently, and quickly as possible in order to ensure continuity of operations as well as minimize disruptions.

At the same time, it is not possible to build an overall, comprehensive picture of activity on the global information infrastructure. Networks themselves are too big, they are growing too quickly, and they are continually being reconfigured and reengineered. As a result, it is essential that strong partnerships be developed between a wide range of stakeholders in order to ensure that the right data are at the right place at the right time.

Creating partnerships for information sharing and coordination is a formidable task. Trust needs to be established among a broad range of parties with varying interests and expectations, procedures for gathering and sharing information need to be developed, and technical issues need to be addressed. Moreover, if the federal government itself is going to be a credible player in response coordination, it needs to have its own systems and assets well protected. This means overcoming significant and pervasive security weaknesses at each of the major federal agencies and instituting governmentwide controls and mechanisms needed to provide effective oversight, guidance, and leadership. Perhaps most importantly, this activity needs to be guided by a comprehensive strategy to ensure that it is effective, to avoid unnecessary duplication of effort, and to maintain continuity.

I would like to discuss each of these challenges in more detail as successfully addressing them is essential to getting the most from information sharing mechanisms currently operating as well as establishing new ones.

Establishing Trust Relationships

A key element to the success of information sharing partnerships is developing trusted relationships among the broad range of stakeholders involved with critical infrastructure protection. (See figure 1 for examples of these stakeholders). Jointly-designed, built, and staffed mechanisms among involved parties is most likely to obtain critical buy-in and acceptance by industry and others. Each partner must ensure the sharing activity is equitable and that it provides a value added to the cost of information sharing. However, this can be difficult in the face of varying interests, concerns, and expectations. The private sector, for example, is motivated by business concerns and profits, whereas the government is driven by national and economic security concerns. These disparate interests can lead to profoundly different views and perceptions about threats, vulnerabilities, and risks, and they can affect the level of risk each party is willing to accept and the costs each is willing to bear.

Moreover, as we testified before this Subcommittee in June,[3] concerns have been raised that industry could potentially face antitrust violations for sharing information with other industry partners, subject their information the Freedom of Information Act (FOIA) disclosures or face potential liability concerns for information shared in good faith. Further, there is a concern that an inadvertent release of confidential business material, such as trade secrets or proprietary information, could damage reputations, lower consumer confidence, hurt competitiveness, and decrease market shares of firms.

Some of these concerns are addressed by this Subcommittee's proposed Cyber Security Information Act of 2000 (H.R. 4246). Specifically, the bill would protect information being provided by the private sector from disclosure by federal entities under FOIA or disclosure to or by any third party. It would prohibit the use of information by any federal and state organization or any third party in any civil actions. And it would enable the President to establish and terminate working groups composed

[3] *Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000* (GAO/T-AIMD-00-229, June 22, 2000).

of federal employees for the purposes of engaging outside organizations in discussions to address and share information about cyber security. By removing these concerns about sharing information on critical infrastructure threats, H.R. 4246 can facilitate private-public partnerships and help spark the dialogue needed to identify threats and vulnerabilities and to develop response strategies.

For several reasons, the private sector may also have reservations about sharing information with law enforcement agencies. For example, law enforcement entities have strict rules regarding evidence in order to preserve its integrity for prosecuting cases. Yet, complying with law enforcement procedures can be costly because it requires training, implementing proper auditing and control mechanisms, and following proper procedures. Additionally, a business may not wish to report an incident if it believes that its image might be tarnished.

For national security reasons, the government itself may be reluctant to share classified information that could be of value to the private sector in deterring or thwarting electronic intrusions and information attacks. Moreover, declassifying and sanitizing such data takes time, which could affect time-critical operations. Nevertheless, until the government provides detailed information on specific threats and vulnerabilities, the private sector will not be able to build a business case to justify information sharing and will likely remain reluctant to share its own information.

Figure 1: Examples of Stakeholders in Information Sharing Efforts

- The public and internet community at large
- Law enforcement
- Government agencies
- The national security and intelligence communities
- Providers of network and other key infrastructure services
- Technology and security product vendors
- Security experts
- Incident response teams
- Education and research communities
- International standard-setting bodies
- Media

Establishing Reporting Needs and Communication Mechanisms

A significant amount of work still needs to be done just in terms of ensuring that the right type of information is being collected and that there are effective and secure mechanisms for collecting, analyzing, and sharing it. This requires agreeing, in advance, on the types of data to be collected and reported as well as on the level of detail. Again, this can be difficult given varying interests and expectations. The private sector, for example, may want specific threat or vulnerability information so that immediate actions can be taken to avert an intrusion. Law enforcement agencies may want specific information on perpetrators and particular aspects of the attack, as well as the intent of the attack and the consequences of or damages due to the attack. At the same time, many computer security professionals may want the technical details that enable a user to compromise a computer system in order to determine how to detect such actions.

After determining what types of information to collect and report, guidelines and procedures need to be established to effectively collect and disseminate data and contact others during an incident. Among other things, this involves identifying the best mechanisms for disseminating advisories and urgent notices, such as e-mail, fax, voice messages, pagers, or cell phones; designating points-of-contact; identifying the specific responsibilities of information-sharing partners; and deciding whether and how information should be shared with outside organizations.

Working through these and other issues has already proven to be a formidable task for some information-sharing organizations. According to the CERT Coordination Center, for example, it has taken years for incident response and security teams to develop comprehensive policies and procedures for their own internal operations because there is little or no experience on which to draw from. Moreover, the incident response team community as a whole is lacking in policies and procedures to support operations among teams. According to the Center, progress typically comes to a halt when teams become overwhelmed by the number of issues that need to be addressed before they can reach agreement on basic factors such as terminology, definitions, and priorities.

Developing Needed Technical Capabilities

Significant resources, knowledge, skills, and abilities clearly need to be brought together to develop mechanisms that can quickly and accurately collect, correlate, and analyze information and coordinate response efforts. But presently, there is a shortage of such expertise. At the federal level, for example, we have observed a number of instances where agency staff did not even have the skills needed to carry out their own computer security responsibilities or to oversee contractor activities. Additionally, according to the CERT Coordination Center, there are not enough suitably trained staff in the incident response community to implement any effective and reliable global incident response infrastructure. The President's *National Plan for Information Systems Protection* recognizes this dilemma and proposes a program to develop a cadre of highly skilled computer science and information security personnel. As this program is implemented, it will be important for the federal government to ensure that capabilities are developed for information sharing and response mechanisms in addition to individual agency computer security programs.

At the federal level, there is also a pressing need for better computer network intrusion detection monitoring systems to detect unauthorized and possible criminal activity both within and across government agencies. Under the President's *National Plan for*

Information Systems Protection, the federal government is working to design and implement highly automated security and intrusion detection capabilities for federal systems. Such systems are to provide (1) intrusion detection monitors on key nodes of agency systems, (2) access and activity rules for authorized users and a scanning program to identify anomalous or suspicious activity, (3) enterprise-wide management programs that can identify what systems are on the network, determine what they are doing, enforce access and activity rules, and potentially apply security upgrades, and (4) techniques to analyze operating system code and other software to determine if malicious code, such as logic bombs, has been installed.

As we testified in February,[4] available tools and methods for analyzing and correlating network traffic are still evolving and cannot yet be relied on to serve as an effective "burglar alarm," as envisioned by the plan. While holding promise for the future, such tools and methods raise many questions regarding technical feasibility, cost-effectiveness, and the appropriate extent of centralized federal oversight. Accordingly, these efforts will merit close congressional oversight as they are implemented.

Making the Federal Government A Model

If our government is going to play a key role in overcoming these challenges and spurring effective information sharing and coordination, it must be a model for information security and critical infrastructure protection, which means having its own

[4] *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection* (GAO/AIMD-00-72, February 1, 2000).

systems and assets adequately protected. Unfortunately, we have a long way to go before we can point to our government as a model for others to emulate. As noted in previous testimonies and reports, virtually every major federal agency has poor computer security. Federal agencies are at risk of having their key systems and information assets compromised or damaged from both computer hackers as well as unauthorized activity by insiders. Recent audits conducted by GAO and agency inspectors general show that 22 of the largest federal agencies have significant computer security weaknesses, ranging from poor controls over access to sensitive systems and data, to poor control over software development and changes, and nonexistent or weak continuity of service plans.

While a number of factors have contributed to weak federal information security, such as insufficient understanding of risks, technical staff shortages, and a lack of system and security architectures, the fundamental underlying problem is poor security program management. Agencies have not established the basic management framework needed to effectively protect their systems. Based on our 1998 study[5] of organizations with superior security programs, such a framework involves managing information security risks through a cycle of risk management activities that include (1) assessing risk and determining protection needs, (2) selecting and implementing cost-effective policies and controls to meet these needs, (3) promoting awareness of policies and controls and of the risks that prompted their adoption, and (4) implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related

[5] *Executive Guide: Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

controls. Additionally, a strong central focal point can help ensure that the major elements of the risk management cycle are carried out and can serve as a communications link among organizational units.

While individual agencies bear primary responsibility for the information security associated with their own operations and assets, there are several areas where governmentwide criteria and requirements also need to be strengthened. Specifically, there is a need for routine, periodic independent audits of agency security programs to provide a basis for measuring agency performance and information for strengthened oversight. There is also a need for more prescriptive guidance regarding the level of protection that is appropriate for agency systems. Additionally, as mentioned earlier, gaps in technical expertise should be addressed.

Developing a Comprehensive Strategy to Ensure Effectiveness and Continuity

A comprehensive, cohesive strategy is needed to ensure that our information security and critical infrastructure protection efforts are effective and that we build on efforts already underway. However, developing and implementing such a strategy will require strong federal leadership. Such leadership will be needed to press individual federal agencies to institute the basic management framework needed to make the federal government a model for critical infrastructure protection and to foster the governmentwide mechanisms needed to facilitate oversight and guidance. In addition, leadership will be needed to ensure that the other challenges discussed today are met.

The *National Plan for Information Systems Protection*is a move towards developing such a framework. However, it does not address a broad range of concerns that go beyond federal efforts to protect the nation's critical cyber-based infrastructures. In particular, the plan does not address the international aspects of critical infrastructure protection or the specific roles industry and state and local governments will play.

The Administration is working toward issuing a new version of the plan this fall that addresses these issues. However, there is no guarantee that this version will be completed by then or that it will be implemented in a timely manner. Additionally, a sound long-term strategy to protect U.S. critical infrastructures depends not only on implementation of our national plan, but on appropriately coordinating our plans with those of other nations, establishing and maintaining a dialogue on issues of mutual importance, and cooperating with other nations and infrastructure owners.

An important element of such a plan will be defining and clarifying the roles and responsibilities of organizations—especially federal entities--serving as central repositories of information or as coordination focal points. As discussed earlier, there are numerous organizations currently collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents, including NIST, the NIPC, FedCIRC, the Critical Information Assurance Office, the federal CIO Council, and various units within the Department of Defense. The varying types of information and analysis that these organizations provide can be useful. However, especially in emergency situations, it is important that federal agencies and others clearly understand the roles of these organizations, which ones they should contact if they want to report a computer-based attack, and which ones they can rely on for information and assistance.

Clarifying organizational responsibilities can also ensure a common understanding of how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals. Moreover, the need for such clear delineation of responsibilities will be even more important as international cooperative relationships in this area mature. If such roles and responsibilities are not clearly defined and coordinated under a comprehensive plan, there is a risk that these efforts will be unfocused, inefficient, and ineffective.

-- -- -- --

In conclusion, a number of positive actions have already been taken to provide a coordinated response to computer security threats. In particular, the federal government is in the process of establishing mechanisms for gathering information on threats, facilitating and coordinating response efforts, sharing information with the private sector, and working to build collaborative partnerships. Other stakeholders are also working to facilitate public-private information sharing on threats in individual sectors and to promote international coordination.

Nevertheless, there are formidable challenges that need to be overcome to strengthen ongoing efforts and to work toward building a more comprehensive and effective information-sharing and coordination infrastructure. In particular, trust needs to be established among a broad range of stakeholders, questions on the mechanics of information sharing and coordination need to be resolved, roles and responsibilities need to be clarified, and technical expertise needs to be developed. Addressing these challenges will require concerted efforts by senior executives—both public and private—as well as technical specialists, law enforcement and national security officials, and providers of network services and other key infrastructure services, among others. Moreover, it will require stronger leadership by the federal government to develop a comprehensive strategy for critical infrastructure protection, work through concerns and barriers to sharing information, and institute the basic management framework needed to make the federal government a model of critical infrastructure protection.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other Members of the Subcommittee may have.

-- -- -- --

We performed our review from July 10 through July 24, 2000, in accordance with generally accepted government auditing standards. For information about this testimony, please contact Jack L. Brock, Jr., at (202) 512-6240. Jean Boltz, Cristina

Chaplain, Mike Gilmore, Danielle Hollomon, Paul Nicholas, and Alicia Sommers made key contributions to this testimony.

(512012)

Mr. HORN. Well, thank you very much. If Mr. Pescatore would join us over there and, staff, see if we could turn around one of those heavy awful tables that we suffer through here, and we have Mr. Molander already at the table. And we are going to move to Mr. Molander. He is the senior researcher for the RAND Corp. that does a lot of good work domestically and foreign. So it is nice of you to appear here.

So where is Mr. Molander? There we are. He moved to the right place to make sure he could get recorded.

STATEMENTS OF ROGER MOLANDER, SENIOR RESEARCH, RAND; AND JOHN PESCATORE, VICE PRESIDENT AND RESEARCH DIRECTOR, NETWORK SECURITY, GARTNER GROUP

Mr. MOLANDER. Thank you, Mr. Chairman. Mr. Chairman and members of the committee, the RAND Corp. has done a large number of studies on the problems that are being addressed here today, including conducting many national and international strategy policy and operational exercises, you might call them cyber war games, in the area of critical infrastructure protection as well as in the cyber crime arena, looking at the impact of the Internet on things like Internet banking, Internet gambling, and the whole impact on money laundering.

My testimony today is a distillation of that experience put together by myself and two RAND colleagues, Robert Anderson and Richard Mesic. In light of the comments that have already been made, I am going to offer a few overview perspectives, hypotheses, lessons learned from about 5 years of doing research in this area.

First, to enable and motivate a more effective dialog between government and the private sector, the government needs, as was mentioned, a specific and much improved framework for targeting the interests of individual infrastructure sectors and companies.

You might say in a sense, Mr. Chairman, it's the private sector that is the key here at the present time. The private sector wants the government to provide threat intelligence, the government wants the private sector to share sensitive vulnerability information. To date neither can or will deliver in a manner that the other deems adequate.

A second point, the companies that are running the critical infrastructure systems all have quite significant risk analyses and contingency plans for various outages and problems; however, for this kind of threat the balance between risk and cost chosen by individual companies may not be deemed best for overall national security interests as judged by the government in carrying out its responsibility. Additional resources are undoubtedly going to be required. This cost gap-filling challenge must be addressed by the Federal Government. The expectation that the private sector will carry all of these costs is terribly misleading.

Third, for those critical infrastructures which are potentially under attack it is prudent to assume that the threat actors, whoever they might be, wherever they might operate, whatever their motivation, are likely to eventually find vulnerabilities. Nature abhors a vacuum. They will be found. We need to assume almost that any major vulnerability will be found by some malevolent actor. To the extent that actions to protect the infrastructure cannot for cost, political or other technical reasons be implemented fully on a day-to-day basis, alert and warning and response systems are critical. Effective AWR, as we call them, architectures are likely to involve a hierarchy of intersected alert and warning systems where the best role for the government probably is to try and take the lead in creating and coordinating almost a system of alert and warning systems and then independently provide sort of motivation for response plans being well vetted and well organized so that people understand what will happen when some alert and warning comes.

The fifth point, any significant attack of a kind that might be characterized as strategic in character would almost certainly be proceeded by various testing and probing activities by the attacking party. This is going to be an ongoing active process, as we have heard. Any data is likely to become dated from an offensive or defensive standpoint, and possibly obsolete quickly. We need to adapt to this kind of dynamic situation.

Six, given our current knowledge base the CIP problem is probably too complex and dynamic at this stage for any single unified strategic concept framework or approach. That means that we have to break the problem down in manageable pieces nationally and internationally and attack the pieces. The kind of unified framework that we would also like to have is something that at best will take place over time.

It is clear, I think, that there is no simple solution silver bullet for enhancing U.S. or global critical infrastructure protection. It is not clear how vulnerable key sectors are, how widespread the effects of a major attack might be, how various responses to that attack, how effective they might be, how well an adversary could marshal the next knowledge and resources to mound a strategic level attack as opposed to what you might call duck bites without extraordinary preparation.

At this time the best approach probably both nationally and internationally is to get down into the details for each individual infrastructure. Every infrastructure is different in terms of their preparation, their risk assessments and their planning. One needs to look at the particular attack modes that are going to be—classes of attack modes that are going to be most troublesome for individual infrastructures, electric power, telecommunications, etc.; the particular generic vulnerabilities that are most worrisome for that sector that can be projected with time even though technology changes; the type and extent of effects of the damages the sector might suffer, the importance to the Nation of those effects, and finally the types and effectiveness of responses that might be expected by the private sector and the government.

Let me reiterate as a close, it is the private sector, Mr. Chairman, that is the real challenge at this point for government.

Thank you.

[The prepared statement of Mr. Molander follows:]

Protecting the Information Infrastructure: A National and International Perspective

Roger C. Molander[1]
RAND

House Testimony
26 July 2000

Introduction

Mr. Chairman and Members of the Subcommittee:

Protecting the information infrastructure is increasingly seen in this city – and looking ahead to the next President and the next Congress, will likely continue to be seen – as one of the highest priority issues the executive branch *and* the Congress face.

To say nothing of the judicial branch looking ahead to some extremely difficult 4th amendment issues.

To say nothing of the future role of state and local governments who could carry much of the responsibility in future infrastructure crises caused by malevolent actors.

And then, and perhaps the true heavyweights in emerging decision-making process, the private sector. Here we are talking primarily about: (1) the U.S. information industry (software, hardware, telecommunications – all of it) as a continuing flagship leader of the information revolution and (2) the owners and operators of U.S. (and U.S.-based multinational) critical infrastructures. The private sector, however, is still a largely inchoate force in terms of the policy and strategy issues on the table.

And finally there's the international dimension – where it is clear that it is imperative that a country accompany its thinking about a national information infrastructure security strategy with comparably fundamental thinking about a set of *regional* and often *global* information infrastructure security strategy and policy issues. Further complicating the situation there are no obvious forums to go to in order to take up the international issues.

That's why we are all just getting started in dealing with the problems associated with protecting the information infrastructure – there are simply a tremendous number of actors and equities involved.

In this environment RAND has done a large number of studies on these problems, including conducting many national and international strategy and policy exercises in the area of critical infrastructure protection. My testimony today is a distillation of that

[1] This testimony is a distillation by the author and RAND colleagues Robert Anderson and Richard Mesic of lessons learned in RAND's research efforts to date on national and international dimensions of the information infrastructure security problem. This testimony represents the authors' personal views and does not in any way reflect the views of RAND or its sponsors.

experience put together in collaboration with two RAND colleagues, Robert Anderson and Richard Mesic.

You should view the points I am about to make as a set of hypotheses about a very complex and challenging problem that this country and world is just beginning to come to grips with. Think of it as the background and rationale for action, for example, to pursue a well-funded and coordinated national *public-private* research program in infrastructure protection.

Background

The rapid development and explosive expansion in use of information technologies very likely provides the past decade's greatest promise for the United States' continued growth and well-being: personal computers on most workplace desktops, linked into corporate information networks; an Internet serving as common communication backbone both nationally and worldwide; wireless communication enabling widespread use of cellular telephones and computing devices; the World Wide Web and electronic commerce providing signs of – and the promise of further – substantial productivity enhancement. In the great majority of these technologies and applications, U.S. firms provide leadership, standards, and jobs.

The information sector in the American economy increasingly provides vital backbone systems upon which our financial, energy, transportation, defense, and telecommunication infrastructures depend. Those systems are becoming ever more interlinked – primarily by the Internet and the public telecommunication network – into the worldwide "cyberspace." And therein lies a major source of increasing vulnerability to the America's economy and its critical military systems: The dependence on these systems is so strong, and the existing vulnerabilities so pervasive, that enhancing the resilience of these infrastructure information systems is a vital national concern.

The vulnerability of United States critical infrastructures has undergone substantial study by the President's Commission on Critical Infrastructure Protection, leading to a number of subsequent actions and reports, such as Presidential Decision Directive 63 and the recent (January 2000) *National Plan for Information Systems Protection* issued by the White House. These studies and documents form a reasonable basis for progress, but must overcome a major stumbling block: Most of the relevant infrastructures (e.g., in energy, telecommunications, transportation, finance) within the United States are controlled by private, increasingly multinational, companies. For a variety of valid reasons these companies are reluctant to share information (e.g., about vulnerabilities, attacks, losses, risk assessments, etc.) with the government, and in turn the government finds it difficult to share information – often classified – about threats with the private sector. These problems of cooperation are difficult, but as a very high national priority they must be overcome if the safety and security of the United States is to be assured.

While we figure out how to solve such national problems we must at the same time look to the international decision-making environment on information infrastructure security where we know that coordinated regional and global action is imperative. Consider U.S. and Canadian electric power and telecom infrastructure linkages and dependencies and then apply that to Europe.

Key Hypotheses

In this environment we have had substantial experience and proffer the following set of hypotheses.

H1. To enable and motivate a more effective dialogue between government and private sector, the government needs a more specific, tangible, meaningful issue framework targeted to interests of individual infrastructure sectors and companies. At present, the "dialogue" primarily involves the private sector asking the government for "threat intelligence" and the government asking the private sector to share sensitive "vulnerability" information. To date neither side can or will deliver in a manner that the other deems adequate.

H2. A lot of "bad stuff" can happen in cyberspace to affect critical infrastructures. But representative examples of bad stuff that can happen exist – in specific infrastructures and systems – resulting from human error, actions of hackers, natural occurrences (fires, earthquakes, hurricanes), and so on. They have not, perhaps, however, happened at a *scale* that *may be possible* and that might have more significant (even "strategic") effects.

H3. The companies running almost all critical infrastructure systems have already developed quite significant risk analyses and contingency plans to meet various outages and problems. However, the *balance* between risk and cost chosen by these individual companies and sectors (even with the advent of sector-specific information sharing and analysis centers) may not be deemed best for overall national interests by the U.S. government. Thus additional resources might be required beyond what is reasonable and prudent from the parochial perspectives of a particular sector – a "gap filling" challenge that could be one basis for a more effective government/private sector dialogue.

H4. Any country that is pursuing offensive information operations must be developing information and models that will be useful from a defensive perspective. Unfortunately, the converse is also true (viz., that defensive efforts point to vulnerabilities that, if not addressed, could be used in offensive operations against the defender). Offensive and defensive IO are opposite sides of the same coin – at some point further progress in both will require close cooperation and understanding between these communities. This may complicate the problem of establishing and sustaining an effective government/private sector CIP dialogue.

H5. For critical infrastructures, it is prudent to assume that "threats actors" (whoever they might be, wherever they operate, and whatever their motivation), are likely eventually to find "vulnerabilities." So, for defensive purposes, "threats" are the same as "risks." That is, since there is widespread cyber capability extant in the world, and widespread motivation by various parties at various times to take advantage of vulnerabilities by using cyber capabilities, we should assume that any vulnerability that constitutes a serious risk basically equates with a threat (of unspecified bad actors exploiting that vulnerability to maximum advantage).

H6. To the extent that actions to protect the infrastructures cannot – for cost, technical, or political reasons – be implemented fully on a day-to-day basis (viz., irrespective of specific threat actions), determining and institutionalizing appropriate systems and procedures for alert, warning, and response (AWR) to attacks naturally becomes a CIP focus. AWR implies plans, procedures, and systems to: (1) assess the nature (including, if possible, perpetrator identity, location, and intent), methods, and likely effects of attacks on the infrastructure(s) and (2) effect timely responses to mitigate the negative effects of the attack. Effective AWR architectures are likely to involve a hierarchy of interconnected AWR systems where perhaps the best role for the national government is to take the lead in creating a "system-of-systems" and coordinating individual corporate and sector-specific AWR activities.

H7. Alert and warning systems and levels *must* be driven by the appropriate *response*. If you have no adequate response to a cyber effect (that can happen in milliseconds), then alert and warning cannot do much good. One should first determine, for specific cyber stimuli that attack specific vulnerabilities, what an organization's response options are – and from those, determine appropriate levels, amounts, and kinds of alert and warning to be instituted.

H8. Any *significant* attack on major portions of the US critical infrastructure would be preceded by various testing and probing activities by the attacking party. This is likely to be an ongoing, active process, because any such data would become dated and possibly obsolete quickly (which could, in the end, be the limiting factor in offensive Information Operations). One must institute a responsive process to adapt to (and, possibly, to exploit defensively – e.g., through the use of deception) various patterns of precursor probes and tests as they evolve.

H9. Given our current knowledge base the CIP problem is too complex and dynamic to be handled (at least initially) by any single unified strategic concept and approach. In this context the best approach is to find a temporary framework that breaks the overall problem into more manageable pieces (as a minimum to establish the possible location or creation of a relevant decision-making process), attack the pieces, and look to a unified and temporally more stable national and international CIP strategy and framework/solution space to take shape over time.

H10. It is necessary that we carefully study an elaborated set of cyber stimuli (attack modes), applied to specific vulnerabilities, leading to specific elaborated effects, and associated relevant responses. These studies must often be both infrastructure sector specific and inter-infrastructure because of greatly varying system architectures, dependencies, and effects across the differing infrastructure sectors.

H11. Political-military context is important. The effects of an attack on one or more critical infrastructures can vary greatly depending on whether the United States is in "steady state," or, for example, is in the midst of a major overseas troop deployment. In the former case, the effects are likely to be somewhat localized, not unlike the effects of a major hurricane or earthquake. In the latter case, it is conceivable that key portions of a deployment might be delayed for up to several days or more, resulting in a possible altered (degraded) military or political situation.

H12. The studies of attack modes, vulnerabilities, effects, and responses mentioned in H10, above, must be based on focused discussions between government and the private sector firms that operate much of the U.S. critical infrastructure. Such discussions would be greatly enhanced if government came with an understanding of the attack modes most relevant to a particular infrastructure sector and the specific vulnerabilities of that sector – having then studied the likely effects of, and range of possible responses to, a strategic-level attack upon that sector capitalizing on those vulnerabilities.

H13. While CIP problems are global, and many critical infrastructures are controlled by international corporations, it is reasonable to *begin* to approach the problem domestically *and* with U.S.-based multinational infrastructure owners and operators. As international issues emerge, they can then be addressed multilaterally with a better understanding of and perspective on domestic interests and constraints.

Conclusions

It should be clear from the above discussion that there is no simple "silver bullet" for enhancing U.S. or global critical information infrastructure protection, or even more broadly, information infrastructure-based critical infrastructures such as electric power. It is still quite unclear how vulnerable key sectors are, how widespread the effects of a major strategic attack might be, and how effective various responses to that attack – such as work-arounds and reconstitution – might be. It is also unclear how well an adversary (e.g., a nation-state or major terrorist group) could marshal the necessary knowledge and resources to mount a strategic-level attack, especially without its preparations and probes being detected.

Given this state of considerable uncertainty, the best approach at the U.S. national level is to consider and refine hypotheses such as we've outlined in this testimony. This process will eventually require analysts and policy makers to get "down into the details" for each critical infrastructure sector. This should lead to a clearer, more focused understanding of the particular attack modes that might be most troublesome, the particular generic vulnerabilities that are most worrisome for that sector, the expected type and extent of effects that the sector might suffer, the importance (to the nation) and costs that might be incurred by those effects, and the types and effectiveness of responses that might be expected (by the private sector and by the government). The government might then be prepared to enter into tangible, specific dialogues with relevant sector providers about these data, at a level of detail that can engage the interest of those providers.

Mr. HORN. Well, we thank you and your colleagues for that fine presentation.

Mr. John Pescatore is the vice president and research director, Network Security for the Gartner Group.

Mr. PESCATORE. Good morning and thank you, Mr. Chairman and the committee, for this opportunity. It looks like I am batting cleanup here. You have heard from a lot of constituencies. In my 22 years working in information security, I have actually worked for the Intelligence Community, the law enforcement community, private industry, in developing fire walls and public key encryption, and now with Gartner Group, working with thousands of our clients across the world addressing their security problems.

Add the citizens to the stakeholders in this, and it is a complex problem, and the key is sharing across those communities. The Internet definitely rewards sharing, it actively rejects attempts at hierarchal command and control and routes around them, to paraphrase a famous Internet saying. What within this mix can the government do to facilitate sharing is the key issue we have touched on I think in a number of ways here.

First, we have heard several times, and I will certainly second it, that the government should first clean up its own act in computer systems and make sure that government computer systems are secure and well managed. We've seen an explosion in use—business use of the Internet that really vastly outpaces the growth of crime against the business use of the Internet today. We see companies like Cisco and Intel and Intuit getting the majority of their revenues through sales over the Internet. They figured out how to do it securely and still run leading businesses.

So the solutions, the technologies and the processes are there. They need to be emulated and replicated across all systems, and government systems are a prime example. We estimate it takes anywhere from three to five times more effort, more total cost of ownership to secure an Internet exposed application than one that has traditionally been inside a closed environment. If you use today's point solutions and antiquated processes that we see many government agencies trying to use, if you use architectural solutions, redefined, reengineered processes, those costs can be halved and become much closer to what it takes to do so behind the fire wall.

So first point, government effort to secure government systems, that is one key inhibitor to private industry willing to share the threat information with the Federal Government. Will it be protected when it is stored by the Federal Government?

Second key point, the government certainly plays a role in defining security standards and can put its buying power behind those standards. We see the National Institute of Standards and Technology [NIST], with the National Information Assurance Program putting together protection profiles for various technologies and systems. Some very good efforts there. Not quite working on Internet time, more bureaucratic time; need to move up to Internet speeds, and not quite so focused on a prioritized list of what makes the most sense to e-business and the needs of all these various constituencies. I think that can be improved.

The government can certainly learn some lessons from what it did in the Y2K period. There were many things that others put together for Y2K; for example, in the National Security Telecommunications Advisory Council [NSTAC], is an example of a very workable way of sharing threat information between private industry on the critical infrastructure side and the government. Did a lot of good work for Y2K.

Another suggestion that we have, we saw the Securities and Exchange Commission require publicly traded companies issue Y2K status information in their quarterly and annual reports. Let's see that for security information. Let's see the government help make security part of the bottom line versus an afterthought for many of these companies. I think that would go a long way.

I want to point out we don't see a need for more alphabet soup of committees and task forces to address this problem or coordinate this problem. We see plenty of those. We see many successful examples, things like the Forum of Incident Response Security Teams, the Carnegie-Mellon Computer Emergency Response Team, things starting up in the Federal Government like FedCERT to share information. We have enough mechanisms. We need to move them forward and increase sharing.

I will sum up, with that buzzer going off, to say we see a lot of successful use of the Internet increase the bottom line of companies, make things more convenient for citizens. Certainly we know cyber crime and information warfare will follow and it will require leadership by the government to address those. I think the government can learn from what private industry has done successfully and adopt best practices on government systems and sponsor leading practices and standards that will apply across the infrastructure. Thanks for your time.

[The prepared statement of Mr. Pescatore follows:]

Statement to the Subcommittee on Government Management, Information, and Technology

26 July 2000
John Pescatore
VP and Research Director, Network Security
Gartner Group, Inc.

Thank you for this opportunity to address an issue that is of critical importance to industry, citizens and government organizations across the country and the world. Given how important use of the Internet has become to all of these parties, coordinated efforts to increase the security of business processes and technologies are critical to continued productivity gains and growth in the Internet economy.

Using public networks like the Internet for critical business processes requires greatly increased security rigor, in both processes and technology. Gartner Group estimates that it is three to five times more expensive to secure an application that is exposed to the Internet than the same application running on a closed network, if point solutions and ad hoc processes are used. By using architectural solutions and re-defined processes, the cost of security can be halved. We have long advised our clients that one of the most critical security processes to reengineer for Internet connected systems is Incident Reporting and Response. Business such as Cisco and Intel, which now make the majority of their revenue by selling to businesses over the Internet, are examples of companies who have thoroughly upgraded their processes for security monitoring and reporting.

There are a number of ways the Government can help create more coordinated responses to computer and network security incidents. The first is by assuring that all Government computer systems are secure and well managed. The Government should be a model citizen on the Internet - but it is currently far from it. While it was business as usual during the Year 2000 rollover period for most private industry computer systems, many Government (both civilian and DoD) computer systems were shut down or disconnected from the Internet to avoid security problems. During the recent ILU virus attack, threat information seemed to flow much more slowly through Government reporting mechanisms than in private industry. The US Government needs to step up its efforts to be a leader in operational security not a laggard. This requires increase training of government security personnel and increased coordination between Government agencies.

The Government can also define security standards and use its buying power to make those standards meaningful in the market. While the National Institute of Standards and Technologies has a program (NIAP) to define standard protection profiles for security products and technologies, there has been little effort made to move this process on "Internet time" or to require Government agencies to buy products that have been tested to these profiles. By committing the resources to produce timely, targeted Protection Profiles and using them as the basis for government procurements, the government can be a market maker.

The government can also take heed of lessons learned during Y2K preparations and used mechanisms (such as the National Security Telecommunications Advisory Council) as models for how to spur sharing of security incident information. There is no need to create a new "alphabet soup" of competing Government agencies and task forces to attempt to collect and distribute incident and threat information - there are numerous working mechanisms such as NSTAC which have already proven their merit. The Government can also learn from private industry, where industry groups such as Acord (in the insurance industry), BITS (in the banking industry), the Forum of Incident Response Teams, and best practice groups such as those run by Gartner Group provide rich mechanisms for industry to share security information.

A reporting regulation that was used during the pre-Y2K timeframe could also be used to great effect for on-going security reporting: require public companies to publish information security status information in their quarterly and annual reports. By increasing the importance of security to the boards of directors of corporations, the US Government can drive security to become a part of the bottom line, versus an afterthought. In countries such as Germany, regulations making directors personally liable for security incidents has resulted in greatly increased attention to system-level security solutions.

By any realistic analysis, the increase of business use of the Internet greatly outpaces the rate of successful security attacks - industry is by and large doing a thorough, credible job of protecting their information systems. However, as business increases on the Internet, more sophisticated criminal attacks will follow. By being a model citizen on the Internet, listening to private industry to discover what already works and by avoiding the temptation to force hierarchical solutions on the inherently distributed Internet, the Government can play a leadership role in making the Internet safe for business and government use.

Thank you for your attention.

Mr. HORN. Thank you very much. We will begin the questioning with the ranking member, Mr. Turner. Each of us will take 10 minutes. And as you can see by the ruckus on the bells, we have another vote so we will both have to get there. But we will get started here with 10 minutes to the gentleman from Texas.

Mr. TURNER. Thank you, Mr. Chairman. Mr. Pescatore, I wanted to followup with you. You made a comment there that we did not need any more task forces or study groups, and then you also made a comment that we had the necessary entities. You referred to the Carnegie-Mellon Institute. I guess it is a similar operation to what we do at the Federal level. Did I gather you said those were sufficient that we had in place?

Mr. PESCATORE. Well, we have the mechanisms, things like CERT teams and FIRST and across DOD and the civilian government and private industry for sharing the—for coordinating response. We need a number of things to help make information sharing easier. Many have been addressed in the testimony. Things like the Freedom of Information Act being addressed to make sure that information shared will stay private, will not be releasable. Making sure information sharing is bidirectional between these communities as much as possible.

So there are ways that we can increase the sharing between these mechanisms, but I don't think we need more mechanisms.

Mr. TURNER. We have a number of people here from various countries around the world. What would you see as the greater need internationally in this area? We all talk about and everybody has mentioned we need greater cooperation. What does that translate into in terms of actual activity?

Mr. PESCATORE. Well, I think what you see the most need for is increased communication between the different layered communities. For example, Interpol between law enforcement, the various NATO and other mechanisms between DOD, and there are existing mechanisms like FIRST that interoperate between companies across countries. The flow between those three communities is near zero. That needs to be increased. And the mechanisms are there, again, but the oomph behind them is not.

Mr. TURNER. I was interested, Mr. Molander, in your comment. You said the problem is the private sector, not the government, and yet I get the impression from listening to the testimony that the government is increasingly going to be required to play a greater role, that the private sector is going to basically say there is a point beyond which we don't really want to go. We don't want to spend the money to go further, but that our national security needs will require us to go further.

So you might want to expand on that thought a little more because I was getting the impression earlier that the direction that we needed to take was that we are going to have to recognize that the government is going to have a greater responsibility, not a lesser responsibility.

Mr. MOLANDER. I think that is probably right. But in the end, I think the real challenge right now is to bring the private sector to the table in seeking solutions to this problem. As yet, the kind of information that we would like to get from the private sector in terms of, for example, the kinds of probes that they are seeing right now, how they are organizing themselves for responding to certain kinds of attacks, classes of vulnerabilities that they can see from their own experience with natural sort of events and things of this character, these kinds of things have not yet been part of a dialog between the government and the private sector largely because the government has not been successful in making the case—and it's not an easy case to make at this early stage—that there is out there perking along, you might say, the kind of strategic threat capability that truly would be more than just a cause for the kinds of problems that we saw with the "ILOVEYOU" virus and things of this character.

The private sector is, if you will, the frontier. That is where things are happening in terms of attacks against the infrastructures, more so perhaps than the attacks against the Defense Department. The private sector—all boats have to get in and start rising here, but the private sector is really missing in terms of aggressive participant in the larger strategic challenge.

Mr. TURNER. What's it going to take to get the private sector to move more rapidly in terms of their willingness to cooperate?

Mr. MOLANDER. Other people could comment on that as well, but I would say a persuasive case made by the government, barring some actual events, of the kinds of vulnerability that the private sector sees could be exploited by a malevolent actor who you might say catches up with the information revolution and catches up with the software and what not, changes that are being made by the infrastructure. So you might think of this as somebody doing a high speed merge, the malevolent actors doing a high speed merge on the highway. But the threat is that they will catch up and the kinds of dialog where the government makes a persuasive case for threat really haven't taken place yet.

Mr. TURNER. I'm not sure we do understand the threat, and maybe we need to have more opportunities for experts like we have on this panel to tell us the worst case scenarios that might be out there for us. We have two panelists here from the Department of Defense, but when we talk in terms of national defense we usually can identify the threat and talk about it. Sometimes we talk about it in top secret meetings, but we talk about it and that's what we try to address.

Maybe we don't have a good perception of the real threat. Do any of you, particularly panelists from the Department of Defense, have any suggestions on how we might better educate ourselves on the nature of the threat? Mr. Vatis with the FBI, I'm sure you have some thoughts on that you could share with us.

Mr. VATIS. I think I agree with the point that one of the things we need to do is to raise awareness about the nature of the threat. And, in fact, a lot of that has been going on. We have provided numerous briefings to different committees of Congress and also to many different parts of the private sector. As one example, I've provided a classified briefing to the owners and operators of the electrical power infrastructure because of their centrality to the functioning of all the other infrastructures. And I think those briefings, as well as real live events such as the various viruses that we have seen and denial of service attacks, have all done a great deal to raise the level of awareness. And I think they've contributed to the progress that actually has occurred over the last 2 years in terms of the private sector taking steps that it hadn't taken before to secure its systems.

But I think all the awareness raising in the world is only going to get you so far. And then you still run up against the fact that companies are not going to do anything until they see that it's necessary to protect their bottom line and their ability to make profits. And I think companies are going to make different decisions about the probability of something happening. They will look at the cost of taking steps to prevent it from happening versus the cost of something happening, discounted by the probability and going through that sort of cost-benefit analysis. And so I think that's really where we need to make progress.

The other thing that I see happening is a bit of a free rider problem. That especially affects the whole problem of information sharing. There has been a lot of talk for 2 and more years about the importance of information sharing. We have set up numerous mechanisms, some of the ones that Mr. Pescatore has mentioned as well as ones that the government has set up, including through the NIPC, to share information from the government to the private sector. And that's all been going on.

But what's principally been lacking, I think, is information coming from the private sector to the government and information being shared among private sector companies. The free rider problem that I mentioned comes from the fact that companies are willing to get information that might help them become aware of vulnerabilities, but they're very wary of sharing their own vulnerability information, not just with the government but with their competitors in industry, because companies see a possible competitive advantage if they're aware of a vulnerability and others aren't. And so that's where I see the principal hindrance to information sharing.

Mr. HORN. I will have to interject now. At 12:25, we go into a formal recess. We will be back at 2 o'clock for the questioning. Other Members will be here. And I believe your host, the Federal Bureau of Investigation, already has other things for you to do during this period. So we are now recessed formally. If you want to ask some more questions fine, but you can also ask them at 2 p.m.

[Recess.]

Mr. HORN. The recess is over, and I hope you had a good lunch, and we thank the Federal Bureau of Investigation for that hospitality. Since none of us on Capitol Hill except the Speaker have a representational allowance, we don't have any.

But let us ask a few questions. We won't keep you that long but there are a few things we did want to talk about.

To the Department of Defense, let me ask this. Has the lack of an international policy on critical infrastructure protection impeded the Defense Department's efforts to address mutual concerns on infrastructure protection? How would you answer that?

Mr. SCHAEFFER. No, sir, I believe that with respect to our international partners we have worked on an individual basis to ensure that where we are reliant upon the infrastructure of the nations where we reside. That is not to say that all the problems are fixed and everything is wonderful, but we are working U.S.-to-host nation to address those issues.

Mr. HORN. In an unclassified setting, can you tell us what countries do you see as having the most developed information warfare and computer attack capabilities?

Mr. SCHAEFFER. I cannot address that in this forum, sir. Actually, that question would probably be addressed better to a member of the Intelligence Community than to this portion of the Department of Defense.

Mr. HORN. We will have Mr. Goss ask that.

How concerned are you in the Defense Department about the proliferation of weapons of mass destruction, viruses, hacking, exploited denial of service, and will increased information sharing improve the response posture of the United States?

Mr. SCHAEFFER. Well, sir, I believe I can state categorically that we're very concerned. Certainly as one can read in the paper every day, the Department is subjected to a substantial number of probes, attempted intrusions, attacks, however one wants to categorize that. Last year, or in 1999, the Joint Task Force-Computer Network Defense registered over 22,000 attacks on DOD systems.

Now, it's very, very difficult to say what portion of those came from within the United States, what portion may have been foreign sponsored, which portion may have been foreign generated. I mean, there's a number of those situations that we continue to pursue.

But the volume and the anonymity with which an attacker can operate unimpeded from around the world sort of states the situation that we are dealing with.

Mr. HORN. In my opening statement, I referred to NATO as a possibility to be able to share information in this area. To what degree—well, let's put it this way. The European Parliament, the various sovereign nation parliaments, and the Council of Europe and all of those groups, everything, the OECD, all overlap each other. But I wondered, since NATO has a working relationship, and one of the reasons was to have a defense group in relation to the Western world, so to what extent, if any, is NATO involved in cyber attack problems?

Mr. SCHAEFFER. In March 1998, Dr. John Hamre made a visit to NATO. We actually visited several individual nations and NATO as a body, the C–3 board, within the NATO structure. And we gave several presentations on U.S. experiences in the area of cyber issues, problems. We laid out our experiences in our own exercise environment, Eligible Receiver 97, which was really the watershed event that got the Department's attention.

Mr. Vatis spoke briefly to the Solar Sunrise incident, which I refer to as a live fire exercise, and we shared those experiences with our NATO partners.

Subsequent to that, we have continued to expand our relationship in terms of sharing experiences, training material, approaches to address information assurance issues both with NATO nations and non-NATO nations as well. We have done that DOD to MOD, the Ministries of Defense of the various nations. And so our relationships have been constrained pretty much within the context of our military partners.

In some cases, some nations have sent non-MOD delegations to DOD to get our perspectives on critical infrastructure issues, information assurance issues, and the Department's approach at dealing with those.

So, I think since the March 1998 timeframe, we've had substantial interaction with our foreign allies and partners to try to convey what we see as rather substantial problems. And I'm pleased to see the progress that NATO has actually made in addressing a number of these issues. Again, there's a long way to go, but it begins with awareness and understanding and common appreciation of the problems.

Mr. HORN. Now, what do we do for those countries that are not in NATO and that rim on the NATO alliance? How do we deal with that?

Mr. SCHAEFFER. We have, on a bilateral basis, exchanged understanding of issues, problems, approaches, with non-NATO nations within Europe. But we've done that again, DOD to MOD. Sweden is an example of a non-NATO nation that we've had information exchanges with.

Mr. HORN. Are the French now in or out of NATO?

Mr. SCHAEFFER. The French are in NATO. And we've had exchanges with them as well.

Mr. HORN. OK. Mr. Genis said this morning, and I'm just wondering what the reaction is of all of you, the suggestion of an international coordination center. Is there an existing organization suited for that purpose? We have a lot of League of Nations groups in Geneva and other parts of Europe and other parts of the world, and we have U.N. possibilities and all that. But I'm just curious if we can go down the line and where do we see for having an international coordination center where you could relate to them and they would keep up on a lot of this and share information. Mr. Reksna.

Mr. VATIS. If I may, Mr. Chairman, I think Mr. Reksna would rather pass on this, if that is OK with you.

Mr. HORN. That's fine, but if he has some thoughts we would welcome them. Because we need to have countries involved, no matter what their size. They're important people to us.

Mr. REKSNA. Actually, we should think always the possibility, if it's possible, we would answer you in a return letter.

Mr. HORN. Well, thank you. Mr. Vatis.

Mr. VATIS. I think the need for a much more efficient and quick mechanism for sharing information internationally is apparent. That is one of the things that the G–8's High-tech Crime Subgroup has been discussing over the last year or two. The problem that we bump up against is that of national sovereignty and the fact that countries are not willing to let foreign law enforcement agencies conduct investigative activities within their own borders for national sovereignty reasons.

And so what the G–8 has been trying to do is come up with a system where countries at least agree to freeze information at the request of another country, and then let the normal mutual legal assistance treaty process take effect. As some of my colleagues had mentioned this morning, that is typically a lengthy process, because in the past in traditional crimes, speed was not always of the essence the way it is in cyber crimes. And so it wasn't of great concern to people that requests would take weeks and months.

Now when evidence can be lost, that sort of delay is simply not tolerable and so we are trying to come up with methods, first within the G–8 and then on a broader scale once we have a model developed, to try and share information more quickly.

But the idea of a single international body that would have powers that might transcend national sovereignty I think would pose difficulties not just for the United States but for most countries.

Mr. HORN. Mr. Kronqvist, any thoughts on this?

Mr. KRONQVIST. Thank you. I think such kind of center should be very useful. But as a law enforcement person, I would like to express that participation of law enforcement agencies should be very manifest and I think probably should be by law enforcement organizations so secure handling of information would not come in the wrong hands.

Mr. HORN. Mr. Juergen Maurer.

Mr. MAURER. I'm not convinced that there is a need for a specific institution to be established. If it comes to law enforcement, I think it would be a much better way to use the existing channels and make them aware of the specific needs. Especially when it comes to Europe, we have to face how many years you need to establish a new police institution, for example, like Europol, and it will need another 10 years to have a real operative institution. So I would prefer to stick with the existing channels and use these channels.

Mr. HORN. Mr. Meneses, what is your thinking on this?

Mr. MENESES. Your Honor, I think Interpol is a good bureau within which law enforcement could properly coordinate and cooperate, considering that it is already existing. I believe what is already needed is to refocus some of these people to concentrate especially on cyber intrusions. They should be given—these people should be directed by the leaders that priority should be given on cases under investigation, especially on cyber intrusions.

Mr. HORN. Thank you. Mr. Genis.

Mr. GENIS. Well, ditto. And I'd like to mention that Interpol would be an appropriate body. But it should be more similar to the NIPC, but which would have control over European countries and other countries than within the United States.

Mr. HORN. Mr. Adamson.

Mr. ADAMSON. Yes, Mr. Chairman, Interpol does have the framework to do this, but what they are lacking is the resources and expertise. There are about 300 police officers from around the world assigned to the General Secretary at Lyon, including 10 Americans. But cyber crimes is just something that has started. Interpol has always been years behind. I think with the new Secretary General coming this year with a renewed interest in Interpol by the United States, and renewed interest by all the first world countries, I think things could change. The framework is there and you still have the sovereignty aspect but at least the framework for communications is there.

Mr. HORN. Mr. Schaeffer, any other thoughts on this?

Mr. SCHAEFFER. Mr. Chairman, I think the only thing I would add is that while existing organizations and mechanisms—or mechanisms do exist, I think we are a long way from a consistent taxonomy in an international sense. What is an attack? What constitutes an attack? What is an event? What is an intrusion? And so I think there is work that has to be done there before we could vest the responsibility for coordination in any one body or any group of organizations. I think there is much that could be done to create a consistent view of the problem and then some sort of international convention of what gets reported, how, and in what context.

Mr. HORN. Mr. Balakgie, is the Defense Department unified?

Mr. BALAKGIE. Absolutely, sir. I would say that there might be some information that would be difficult to share but that's my intelligence. I think you're talking about certain levels where you know something is going on, sharing of information needs to be done in a rapid manner. It's what happens before you get to that point that I think is challenging for us.

Mr. HORN. Mr. Brock, any thoughts on that, looking around the world and around the United States?

Mr. BROCK. I think there is a need for more international sharing. I think at least initially it would be difficult to see one body doing that initially. Much as in the Y2K, people that have already established trust and working relationships in particular sectors, it might be feasible for them to begin sharing information among themselves and at some point look for opportunities for improving sharing among those different groups.

Mr. HORN. Mr. Molander.

Mr. MOLANDER. I was going to say that same thing. I think Y2K was something special, and those people who paid for it by drinking champagne in paper cups did over the period leading up to that establish a precedent that one could build on even if you can't very quickly even think about how to get started on international law enforcement institutions. I think the precedent set by ICAO and IATA and international ITU should be built on before both personal relationships are lost and the experiences are lost because you can do a lot of work in that area. And as I testified earlier, I think bringing the private sector through the individual infrastructure, treating them independently, into this problem effectively is a very important thing to do. And this would be a good place to start.

Mr. HORN. Mr. Pescatore.

Mr. PESCATORE. I think I will echo one comment I believe Mr. Schaeffer made, that the important piece is the consistent taxonomy and lingua franca for defining what is an incident in different times and we see nascent standards in that area, work within the DOD and private industry, to come up with a common language. That would be the first step to get that in use across these communities and that would facilitate information sharing, be it any of these difference mechanisms that we talked about as a coordinating body.

Mr. HORN. Now the private sector sort of was in and out of your testimony, depending on the situation. Is the private sector here, Europe, Asia, wherever, in computing, are they aware of the problems that the viruses create, are they working on ways to block that in the computers that they sell? You don't have to name any names, if you don't want to. But does that occur somewhere? It seems to me this is a wonderful market for someone if they can figure out how to attract people who are virus experts and all the rest of it. So what's your feeling on that? And do they realize the size of this problem and what it could do to the free world as well as the nonfree world?

Mr. Brock.

Mr. BROCK. Every time I testify on computer security, I get several calls the following day from vendors saying we have the answer and they want to come over and do a demo or whatever. And many of them I think, in fact, do have good products. But the problem that we've seen at the agencies we've reviewed is that using a tool, that many agencies have tools but they don't use them effectively. And that's the secret. You can buy a tool that is very effective and we have gone into agencies where they have great firewalls but they haven't turned on all the features of the firewall, or where they haven't trained the people to use it or they haven't updated it and it is two generations back and viruses and other attack methods have progressed.

So I think there are opportunities. But you just can't use a tool without knowledge of how that tool is supposed to work and without continual training to make it work.

Mr. HORN. Is there any other feeling from those of you that live in Europe as to whether your manufacturing industries see this as a real opportunity, if they can block out the type of viruses or whatever it is? Are they not interested or are they interested in doing this? I think that's where some brain power ought to be given to it. It's like anything in defense, everybody—you get it done, somebody has something that's bigger and then so forth and so on. So it seems to me this would be a very good market for everyone there.

The other thing is do the antitrust laws in the case of the United States, does that keep manufacturers and others from getting in at the top of this problem? And is that type of sharing, should that type of sharing be exempted if it in any way is a problem for the antitrust laws? I don't know the GAO has looked at that and we don't have anybody really from Justice on the legal side. But I think we need to pursue that with the Department of Justice and see if something needs to be done to amend the law.

Mr. BROCK. My colleague, Joe Williamson, testified last month on H.R. 4246, the Cyber Security Information Act, which was very similar to a Y2K legislation that eased some of the concerns that companies had about sharing information so they wouldn't violate various antitrust provisions, and we were very positive about that act and thought that anything that would alleviate concerns between companies about sharing information was a positive step forward.

Mr. HORN. Well, I think you're absolutely right on that and we need to pursue that a little more perhaps with the Judiciary Committee.

Let me just ask on the cyber attacks that have been investigated, is there a single point of contact in the United States that all of you who are not in the United States use as your contact point? Is it the FBI's center or are there other places you can also—Carnegie-Mellon has not really come up this morning and Carnegie-

Mellon has been doing a lot of work on how to deal with this problem.

So I don't know if any people that are—are you primarily relating to Mr. Vatis and the center there? Or are there others that can help you in this country? Because we'd like to know where they are and we know about Carnegie-Mellon. Is there any? Yes?

Mr. MAURER. Our first partner in these cases would be the FBI. If it comes to a legal assistance request, we should have to go through the Department of Justice, but they refer us always then back to the FBI. So our main partner would be the FBI.

Mr. HORN. Is that the general feeling of most of you, that you relate to the FBI essentially? Yes?

Mr. KRONQVIST. Yeah, normally we have contact with the FBI through the Legal Attache's office. But we have also other contacts with them, some of the other parts of the FBI, because we have training exercises with the FBI also on projects like that.

Mr. HORN. Well, they're a good group to deal with. Do each of your countries have decent legislation now to combat the cyber attacks? I know the Philippines has. I wish our Congress could move as fast as yours did, because you seemed to move very rapidly. Is there a model law that would fit for every country on that? I realize there is different legal practices under the laws.

But do you feel that there's some of the countries that maybe surround you don't have any laws on this and maybe some don't even care to have any laws about this, because some of them might be doing the things that we are trying to block. So is there a feeling that there is a weakness of laws in some of your countries? Yes? Dr. Maurer.

Mr. MAURER. I'm not that familiar with this part of our work, but it seems that there's a feeling that there is a lack of the law passage. There is an effort by the European Community to harmonize the different laws. So the European Council or the members of the European Council or delegation located here in Washington, DC, they might be a good place to go and get more information on that.

Mr. HORN. Any other thoughts on that? Well, let's get to the point of should there be a global treaty on this? And does it even make any sense, given all the diversity and all the complexity that's involved in this? Should that be either pursued bilaterally and signing or having the Europeans deal with that, the Asians on their continent, whatever it is? That if a global treaty is needed? What is the feeling on that?

The gentleman from Latvia might want to respond on this one because I would think that would be in your interest in terms of Europe and that area to have some sort of a relationship. Any thoughts on it, as we would say in this institution, the gentleman from—in your case you're the gentleman from Latvia, and we are glad to have you here.

Mr. REKSNA. Without doubt, we'll need agreements on cooperation. But we should say openly that actually all the countries, there is much bureaucracy in each country and any more agreements—any other agreement also like needs more bureaucratic work and papers. In order to solve, to detect a crime, the main thing is time—to shorten the time. And because of that, I would agree to that said by our colleagues that at the present moment, maybe one of the most effective ways to work in this direction is personal contacts, to have more personal contacts and to have really good working relationship and contacts with LEGAT, with FBI liaison officers.

And for sure, there should be present such a thing as trust. Trust as on the level of law enforcement institutions in the country, between different countries, and the trust between—we are to build the trust between the law enforcement agencies and the private sector. Because if there is a trust, there would be an effect.

Mr. HORN. Thank you very much. Mr. Vatis, what do you think on this?

Mr. VATIS. I think one of the most pressing needs internationally is for harmonization. Or if not quite harmonization, at least some minimal level of substantive criminal law in all the countries around the world to specifically address computer crimes because one of the problems that we have seen is if we have an incident and we determine that the perpetrator is located in a country where there is no applicable law, there is no chance for prosecution oftentimes in that country and there is also no chance for them to provide assistance to us because they don't have the legal basis to even engage in an investigation.

But I think our approach has been that the best and most likely way to achieve that gradual creation of laws around the world is not by jumping right to a global treaty of some sort, because I think that would take a considerable amount of time, given the great differences in perspectives and priorities among the different countries, but instead to try to encourage the passage of new laws on a bilateral basis, and on a multilaterally basis first to deal with smaller groups of countries that have common interests.

So we've been doing that through the G–8 and then Europe has been doing that through the Council of Europe. And I think if we start with those types of smaller groups of countries with common interests we'll eventually create some momentum and eventually see most, if not all countries around the world have applicable laws.

Mr. HORN. Any thoughts on this, Mr. Kronqvist?

Mr. KRONQVIST. Yes, I think international agreements can be very useful because even domestic legislation can be organized very rapidly if there is—international work is the issue.

Mr. HORN. Dr. Maurer.

Mr. MAURER. Just would like to support the thoughts Mr. Vatis just told us. That is exactly our position too.

Mr. HORN. Mr. Meneses.

Mr. MENESES. I agree with the observation of the honorable chairman that there should be an international or global treaty, considering that information technology moves so fast. And the Web site would be on the other part of the world and the suspect or the culprit may be on the other side of the world and there may be a problem on how to get some of this evidence. But if everybody—if there is a treaty, at least the investigators or the law enforcers would have a chance to call on such country or nation to give in some of the evidence that we need. Of course the recommendation of Mr. Vatis could also be a preparatory step to that global treaty.

Mr. GENIS. I'd like to stress sir that an international treaty will allow us or will give us the ability to address foreign countries, besides the United States, where we speak in the same legal terms. And it will simply make the process accelerated.

Mr. HORN. Mr. Adamson.

Mr. ADAMSON. Yes, I mentioned that Interpol works with a number of organizations and, as I previously mentioned, the Council of Europe has been doing this with a draft convention on cyber crime recently. And they are putting together, this will probably be the first international treaty to address this problem of cyber crime. As I understand it, the text will be finalized by the end of this year. The Committee of Ministers may adopt it as early as autumn 2001. Again this is piecemeal, this is Europe. But it is the first step probably to do something worldwide.

Mr. HORN. What is the process in terms of Interpol in developing a document such as that?

Mr. ADAMSON. Well, Interpol isn't doing it. Interpol is only supporting it. It is really the Council of Europe. It is again one of the many organizations that we belong to. But we are listening, we are watching what they are doing and perhaps through our mechanism we can show the rest of the world that this can be done.

Mr. HORN. That is good. I am sure that is a publication that will be sought in a lot of places.

Any other thoughts on this?

Mr. ADAMSON. Not from me, no, Mr. Chairman.

Mr. SCHAEFFER. I think I find what Mr. Adamson says very interesting. I wasn't aware that there was such work going on. But I think, from a Department perspective, I think Mr. Vatis articulated our position very well.

Mr. HORN. Well, which reminds me on this situation, if that's so, are our defense attaches educated and trained that this is a real problem? Where in our Embassy should we have somebody that can deal with this?

Mr. SCHAEFFER. I think we are continuing to educate and raise the awareness of the defense attaches around the world. But—there are levels of understanding to the problem and many of the issues that we deal with are down in the nuances of exactly what happened and how and where, and that takes a depth of understanding that is much, much greater than just awareness. We continue to pursue that, but—again, we are a ways away from having a completely trained and educated cadre of folks around the world.

Mr. HORN. Thank you. Any other thoughts?

Mr. BALAKGIE. Just one other comment to the defense attache question. Since they are managed out of a difference intelligence agency, we do have some procedures that they are provided on how to deal and address some cyber issues in terms of their role in the Embassies. So there—just to reinforce that there is an awareness.

On a previous question on an international treaty, I would echo what some of the other panelists have already stated, and that is it would go a long way in at least having the ability to reach into some of these other countries when a problem occurs and see some legal or law enforcement activities kick into gear to help us address some of these issues. So I would definitely think that would be highly recommended.

Mr. HORN. Well, that's a very good point that we cannot wait until it happens, we need to get ahead of the game.

Mr. Brock.

Mr. BROCK. I think you're raising a very interesting point. I think there needs to be all sorts of avenues for international cooperation. And sometimes if you have a good relationship informal things that are flexible work very well when you have a good understanding, but when you don't have a good understanding that sometimes more formal arrangements really force you to lay out the issues in ways of dealing with them.

Another area that could lead to interesting discussions as well, just as you have arrangements, treaty arrangements on weapons of mass destruction for chemical and biological warfare, there might be a point some time where you would want to consider such treaties that would prevent using cyber warfare as a weapon of mass destruction, which it certainly has that capability.

Mr. HORN. It certainly has the capability of scooping up a lot of money in one place or the other also. It is amazing what can be done. Mr. Molander.

Mr. MOLANDER. We have tended to call—use the term "weapons of mass disruption" for the context that Mr. Brock spoke about. I think the proposed convention would go a long way in a dimension that Mr. Schaeffer mentioned, which was get a taxonomy that could be used by someone. There is an extraordinary language problem. One sees it in law enforcement and in critical infrastructure protection. It also will help to get ready for the point where one deals with the difference between is this crime or is this war? And I think that's an interface that is a real challenge for I think every country because every country handles matters differently.

We have a fourth amendment; other countries don't. And the possibility of having an international convention that covers acts of war through or using cyber space was introduced a couple of years ago at the U.N. by the Russians. One of the reasons it probably did not go anywhere is that unlike biological weapons and chemical weapons, where there is an international consensus on not using those weapons as weapons of warfare, there is no such consensus on nuclear weapons. What consensus might emerge on using cyber weapons or whatever you want to call them against infrastructures, for example, is a long way off, and I think until there is some common goal that people can all endorse trying to write a treaty, and we ran an exercise one time that said write me the first article of the treaty, I've had treaty experience. Write me the first article and then tell me what goal that article is going to advance you toward. And that left everyone mute.

Mr. HORN. Well, that reminds me in my university President days, I learned do not be the Alpha project in a computer operation. Go way back and be the last one, the Zebra project. And a lot of our problems in our own domestic government have been because they did not have good management at it and they are constantly reinventing the wheel and this is too dangerous to be reinventing the wheel unless it is going in a decent direction. Mr. Pescatore, any thoughts on this?

Mr. PESCATORE. I would echo the importance of a global treaty or agreement on the difference between crime and warfare. We can certainly spin a scenario of an environmental group in India attacking U.S. banking systems in cyber warfare that appears to come from China, what is the response? Is it crime? Is it warfare? What is the common definition between the two and agreed upon responses? I think that will be a major problem in the future.

Mr. HORN. In our closing here, if there is any questions that any of you would like to ask others while they are here, this is a pretty talented group, so if say the General Accounting Office that works for Congress throughout the world, if you have any questions, Mr. Brock, that we've missed along the line, feel free to ask something, and the same with our guests.

Mr. BROCK. We are actually doing a review of both Mr. Schaeffer's operation and Mr. Vatis's operation now. So we have been exercising our opportunities to introduce them and the results of those should be available next spring, and hopefully we will have another opportunity to share the results of that.

Mr. HORN. We would be glad to see it.

Let me just thank the staff that have helped on this J. Russell George, our staff director, chief counsel. Ben Ritt is to my left, your right, he is on detail to us from the General Accounting Office. Bonnie Heald, director of communications, Bryan Sisk, clerk, Elizabeth Seong, staff assistant, William Ackerly and Davidson Hulfish, interns, and for Mr. Turner's staff, Trey Henderson, counsel, to my right and your left, and Jean Gosa, minority clerk, and Joe Strickland, we thank you and your colleague, Colleen Lynch, our court reporters.

I think that this has been very productive, at least for us, and I hope it has to some degree for you. I thank each of our witnesses today. Some of you have traveled great distances to be here. Your testimony has been very helpful to this subcommittee as we continue our oversight of computer security issues in the United States.

As all of you are aware, the national and international remediation efforts associated with Y2K were well coordinated and highly successful, but that was after congressional oversight when they finally got around to it and it worked out. But this is a situation where you can't drift for the years that we had drifted on Y2K. Y2K provided us with a snapshot of our Nation's interdependence, and intradependence. This soaring number of cyber attacks provides us with an entire photo album and we need the same, in the United States at least, Y2K-type of focus on this issue that we did on that issue.

Each of our governments must have a matrix in place to ensure the security of its critical infrastructure. This subcommittee is in the process of developing a system to gauge the progress of our Federal agencies in protecting their computer systems against these attacks. We will be examining that progress in September.

We have asked the Comptroller General of the United States, who heads the General Accounting Office, to be looking at all of the computers's hardware as well as the software throughout the Federal Government. We are way behind in a lot of computing. We are still in the sixties in some parts, and many of you are way ahead of us.

So each of our governments must have a matrix in place to ensure the security of its critical infrastructures.

This subcommittee is in the process of developing a system, as I said, to gauge the matter, just as we did on Y2K, and when we come back from the August recess we'll be looking at this matter again.

Beyond this domestic challenge, we all must begin addressing the need for well-coordinated, international structure that can provide timely and accurate information to those who need it. On behalf of the subcommittee and the Committee on Government Reform generally, I thank you for your insight, your time, and your participation.

So have a wonderful trip home and we appreciate your coming and spending your talents with us. We are now adjourned.

[Whereupon, at 3:03 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

Subcommittee on Government Management, Information, and Technology
July 26, 2000
"Cyber-crime – Computer Security"

Response to Subcommittee Questions

1. **Can you estimate what percentage of your cases have an international component?**

100% of INTERPOL cases are international. INTERPOL is the only global police organization. It is recognized by, and cooperates with, other leading international organizations including the United Nations, the World Customs Organization, the Council of Europe and the Organization of American States. The Organization also works closely with many non-governmental and private organizations with mutual interests in law enforcement issues and crime prevention. Sixteen U.S. federal and state law enforcement agencies currently detail senior investigative staff to INTERPOL USNCB. Nine of these agencies also detail senior representatives to INTERPOL headquarters in France. All have gained from their investment in the form of increased international law enforcement cooperation and visibility.

As to the role of the U.S. National Central Bureau, it is an important component for U.S. participation in the INTERPOL network. As a condition of membership, each of INTERPOL's 178 Member Countries is required to establish and maintain a National Central Bureau (NCB) to serve as the point of contact for INTERPOL. NCBs are the operational organs of INTERPOL and the means through which the world's law enforcement entities exchange criminal investigative information and provide assistance. NCBs provide a single point of contact for domestic law enforcement components seeking assistance abroad, and for foreign governments trying to identify the authorities they need to contact in the United States.

The structure of U.S. law enforcement differs significantly from that of many INTERPOL countries, where size often dictates a single national police agency. By comparison, the multi-tier U.S. system – with more than 18,000 federal, state and local law enforcement agencies – appears large and fragmented, making it difficult for an outsider to know which department is empowered to deal with a particular matter or to supply information. Facts support this – as of 1998, there were over 83,000 sworn U.S. federal officers with arrest and firearms authority, with more than 50,000 engaged in criminal investigation, police and patrol activities. State and local law enforcement figures add to this complexity – as of June 1997, local police and sheriff departments numbered nearly 700,000 sworn personnel.

These U.S. officers are the USNCB's primary customers, and obtaining the international criminal investigative support they need is our primary mission. The same officers reciprocate with their international police colleagues by providing responses to foreign requests for investigative assistance forwarded from the USNCB – each request complying with U.S. laws and statutory authorities. This interaction with U.S. and foreign law enforcement – coordinating requests and responses for criminal investigative assistance (including translation support) – is the heart of the USNCB's daily business.

The USNCB is unique in U.S. law enforcement, and has been structured to meet the complexity of its mission. In addition to 65 permanent staff, the USNCB relies upon 23 detailed senior investigative staff from 16 U.S. federal and state law enforcement agencies to direct and coordinate domestic and foreign requests for criminal investigative assistance. It has also established a network of State police liaison offices in all 50 states to ensure the proper and timely receipt and response to investigative requests forwarded through state and local law enforcement channels.

As with other criminal matters, domestic law enforcement requests for assistance concerning computer related crimes, are forwarded to the appropriate INTERPOL member country; similarly, foreign requests for U.S. law enforcement assistance on international investigations are forwarded to the U.S. law enforcement component with statutory authority for the matter under investigation.

Unfortunately, statistics in the area of 'cyber crime', whether it be computer related crime, high tech or information technology (IT) crime are unreliable and at best incomplete, simply because the international law enforcement community is working with different definitions and legislation, where legislation is available. Currently, at least 60% of INTERPOL membership lacks the appropriate legislation to deal with Internet/computer-related crime. The result is that such offences are then classified according to their nearest common law derivative. For example, a case involving Internet related child pornography can end up being treated as an ordinary pornography or sexual offence statistic. Another problem is the lack of reporting by private firms due to a fear of the media/PR repercussions.

Regardless of our ability to account for every case of computer-related crime, our focus must be on its far-reaching potential for destructive criminal activity. The ease with which cyber crimes are committed, the multiple jurisdictions of these crimes, the lack of legislation, and the seemingly risk-free environment for the cyber crime perpetrator, are factors that point to a likely increase in this emerging crime type.

2. **How would you rate your cooperation with the Federal Bureau of Investigation's National Infrastructure Protection Center (FBI/NIPC) on cyber intrusion cases?**

   The USNCB cooperates with FBI's NIPC by routing inquiries for criminal investigative assistance it receives from foreign law enforcement components to that FBI unit for resolution. To date referrals to the NIPC on intrusion cases have been limited to a handful of cases.

3. **Could you comment on any past investigations which you worked with the FBI/NIPC?**

   The USNCB has cooperated with the NIPC by forwarding international requests for criminal investigative assistance on cyber crime. Typically, forwarded matters are then resolved by investigating offices who work directly with the requesting country. On the limited number of referrals made to NIPC, we have not received feedback on the final outcome of cases, nor have we received further inquiries from requesting countries indicating that issues were not appropriately handled by NIPC. We are currently exploring new ways of improving cooperative efforts with NIPC.

4. **What measures would be useful to you as investigators regarding record keeping by Internet Service Providers or by victims or cyber intrusions?**

   Because the USNCB is not operational, the actual investigative agencies handling INTERPOL referrals and collateral requests would in a better position to respond to this question. However, through experience gained in working with those agencies, we have noted that investigations are often hampered due to a lack of access to ISP records and transaction logs, or the inadvertent destruction of those records before law enforcement can gain access. Therefore, complete access to those records, authorized by warrant or subpoena, and more stringent record keeping legislation for ISPs, would significantly aid the investigator and help to assist in violator identification.

5. **Regarding training, what training can be done on a national or international basis to improve international response to cyber intrusions?**

   Because of the rapid growth in technology and its expansion to all sectors of society, cyber crime requires an appropriate and concerted effort from U.S. and international law enforcement. U.S. police and agent training courses should include introductory segments familiarizing personnel with cyber crime *methods and the general conduct of relating investigations, to include general computer forensic practices and rules on the handling of computer-related evidence. In addition, advanced courses should be made available to all requesting local, state and federal law enforcement agencies on specific cyber crime areas, and on complex relating matters, such as jurisdiction determination. This type of preparation will help ensure the enforcement response is adequate to the threat.*

Given the inherent international nature of cyber crime activity, law enforcement entities should also be familiar with the INTERPOL network and tools available to link them with the appropriate foreign law enforcement entities quickly and securely. In the area of IT crime, for example, INTERPOL maintains a 24-hour point of contact network comprised of approximately 40 member countries, accessible in each member country through its INTERPOL National Central Bureau. Department of Treasury and Justice new agent training programs now include a mandatory block of INTERPOL training, which introduces new agents to the techniques and strategies in conducting investigations with an international nexus, as well as tools available through the Organization. In the U.S., the USNCB State and Local Liaison Office offers basic INTERPOL training to state and local enforcement entities. Unfortunately these local training programs are heavily dependent upon dwindling financial resources that severely impedes our ability to reach a growing number of state and local police forces.

INTERPOL Headquarters in Lyon, France offers a number of training courses on information technology crime, such as "Computer-based Evidence Operating Systems" and "Computer-based Evidence - the Internet". A 'train the trainer' course is planned for January 2001. In addition, INTERPOL publishes two training manuals on the subject, which are disseminated to its 178 member nations. A training video is currently in production that will be disseminated to all INTERPOL members accompanied by a CD-Rom that will serve as an introduction on how to deal with computer-related crime and evidence. Here too, however, a lack of adequate resources prevents the Organization from keeping pace with this rapidly changing field of crime and from reaching a majority of its members. The governments of France and the U.K. are currently funding INTERPOL computer training initiatives in Africa.

As addressed in the response to Question No. 1, the collection of accurate statistical information on cyber crime cases is difficult at best. INTERPOL and its expert working parties should work to alleviate this problem by setting standards and definitions, and to bring, with the backing of the G8, legislative reality to these standards.

6. **Can you please discuss your working relationship with the private sector in your nation in cases where they are the victims of or unwitting participants in a cyber intrusion?**

INTERPOL considers that it is vital to protect the global business infrastructure on which all economies depend. Recognizing that this infrastructure is at risk from high tech crime and taking into account the extraordinary rate of development of this type of crime and the "frontier-less" environment in which it takes place, it is essential that the public and private sectors work together in strategic alliance to challenge cyber criminals in the most effective ways possible. To that end, INTERPOL maintains sound relationships with a number of private sector concerns and businesses. It is currently exploring whether there may be viable possibilities for closer cooperation and information sharing with private sector firms. However, in order to avoid potential conflicts of interest and comply with all legal requirements on the data security, the preference is to work with the collective industry representatives and/or associations that are adversely affected by this type of crime (e.g., INTERPOL is currently in the process of completing an international training video in partnership with the Internet Alliance).

The USNCB's involvement with the private sector is limited. The vast majority of USNCB cases originate directly from U.S. or foreign law enforcement component requests. Many of the requests concern private companies that become involved in some aspect of crime, and most of the cyber intrusion matters involve private corporations.

7. **Can you discuss current or proposed legislation in your nation for addressing cyber intrusions?**

INTERPOL collaborates closely with a number of organizations, academic and other, involved in projects to collate and evaluate national legislation on computer crime. Their aim is to ultimately develop international standards and best practice measures in the area of cyber crime. One example of this is INTERPOL's work with the Council of Europe to develop a draft convention on cyber crime. Provisionally entitled "Draft Convention on Cyber-Crime", this Council of Europe text will be the first international treaty to address criminal law and procedural aspects of various types of offending behavior directed against computer systems, networks or data, as well as other similar abuses. This legally binding text aims to harmonize national legislation in the field, facilitate investigations and allow efficient levels of co-operation between the authorities of different States. The text should be finalized by a group of experts by December 2000 and the Committee of Ministers could adopt the text and open it for signature as early as Autumn 2001.

INTERPOL is currently finalizing a cooperative agreement with the G-8 Sub-group on High-Tech Crime, aimed at preventing duplication and the resulting waste of resources. It is hoped that this collaboration will result in the political backing for legislative changes to implement international standards and notification procedures through a single point-of-contact contact network.

8. **What means can you suggest for improving the process for obtaining evidence internationally--protected seizures, trans-border search and seizure, computer forensics, etc....?**

   The International Criminal Police Organization has established rules of police cooperation for its 178 Member countries. This framework facilitates and simplifies requests for criminal investigative assistance across borders, and works concurrently with ministerial arrangements for rendering mutual legal assistance.

   Given the proliferation of computer-related crimes and indications that this trend will continue, there is a recognized need to standardize methods of investigation, evidence collection, and forensic examination. Entities involved are making efforts to work within existing Mutual Legal Assistance Treaties and, when necessary, to identify areas where new legislation is required.

9. **What can you suggest to improve our capabilities to locate and identify criminals, and specifically the preservation of critical transactional data and other information that must be shared quickly?**

   The United States can leverage its membership in INTERPOL to help achieve improvement in the location, identification and rendering of criminals and fugitives. The INTERPOL network, connecting all 178 Member countries, is undergoing an upgrade that will permit state-of-the-art notification procedures and enable foreign law enforcement components, working in concert with private industry, to preserve transactional data and share critical information.

   Our ability to deal effectively and efficiently with cyber crime can be enhanced through continued coordination and cooperation among U.S. law enforcement agencies dealing with various aspects of cyber crime, and through competency building for less experienced enforcement agencies worldwide.

   INTERPOL maintains a secure website dedicated to sharing restricted law enforcement information on a variety of crime areas. It is currently working to establish secure access specifically for cyber crime investigators around the world, in order to enable the sharing of information, such as the Computer Crime Manual, in digital format.

10. Based on your own national experience, what can you suggest to other nations regarding governmental organization to detect, warn of, and respond to cyber intrusions?

As cyber crime is inherently international, the major focus should be on developing a broad contact network. However, one's national response in an international case is only as good as the ability and efficacy with which other international players respond. This point underlines the need for thorough competency building exercises and training programs to strengthen the weak links in the network and, in so doing, to develop effective regional responses.

INTERPOL membership and participation increases the likelihood of detection, timely notice and proper law enforcement response to cyber intrusions. It also permits access to a 24-hour network of national experts in approximately 40 countries, in a secure and confidential manner.

Statement for the Record of
Donald M. Kerr
Assistant Director
Federal Bureau of Investigation
Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.
7/24/2000

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the Internet and data interception capabilities developed by the Federal Bureau of Investigation. The use of computers and the Internet is growing rapidly, paralleled by exploitation of computers, networks, and data bases to commit crimes and to harm the safety, security, and privacy of others. Criminals use computers to send child pornography to each other using anonymous, encrypted communications; hackers break into financial service companies systems and steal customer home addresses and credit card information; criminals use the Internet's inexpensive and easy communications to commit large scale fraud on victims all over the world; and terrorist bombers plan their strikes using the Internet. Investigating and deterring such wrongdoing requires tools and techniques designed to work with new evolving computers and network technologies. The systems employed must strike a reasonable balance between competing interests - the privacy interests of telecommunications users, the business interest of service providers, and the duty of government investigators to protect public safety. I would like to discuss how the FBI is meeting this challenge in the area of electronic mail interception.

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search E-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting our Carnivore system as something ominous and raising concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that this topic be discussed openly–and in fact this was the reason we choose to share information about this capability with industry experts several weeks ago. It is critically important as technology, and particularly communications technology, a continues to evolve rapidly, that the public be guaranteed that their government is observing the statutory and constitutional protections which they demand. It is also very important that these discussions be placed into their proper context and that the relevant facts concerning this issue are made clear. I welcome this opportunity to stress that our intercept capabilities are used only after court approval and that they are directed at the most egregious violations of national security and public safety.

The FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), commonly referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". Such federal government interceptions, with the exception of a rarely used "emergency" authority or in cases involving the consent of a participant in the communication, are conducted pursuant to court orders. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated.

Federal surveillance laws apply the Fourth Amendment's dictates concerning reasonable searches and seizures , and include a number of additional provisions which ensure that this investigative technique is used judiciously, with deference to the privacy of intercepted subjects and with deference to the privacy of those who are not the subject of the court order.

For example, unlike search warrants for physically searching a house, under Title III, applications for interception of wire and electronic communications require the authorization of a high-level Department of Justice (DOJ) official before the local United State Attorneys offices can make an application to a federal court. Unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders, instead, the applications are veiwed by federal district court judges. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offenses being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the type of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence–not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are met. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United States Attorney's office handling the case and frequently by the court as well. Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects or others not named in the application.

To ensure the evidentiary integrity of intercepted communications they must be recorded, if possible, on magnetic tape or other devices, so as to protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings must be presented to the federal district court judge and sealed under his or her directions. The presence of the seal is a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

Within a reasonable period of time after the termination of the intercept order, including extension, the judge is obligated by law to ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory, that includes notice of the order the dates during which the interceptions were carried out, and whetehr or not the communication were intercepted. Upon motion, the jusge may also direct that portion of the contents of the intercepted communication be made available to affected person for their inspection.

Under Title III, any person who was a part to an intercepted communication or was a party against whom an interception was directed may in any trial, hearing, or other proceeding move to suppress the contents of any intercepted communication or any evidence derived therefrom if there are grounds demonstrating that the communication was not lawfully intercepted, the order authorizing or approving the interception was insufficient on its face or the interception was not in conformance with the order.

The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, disclosed, or used, may recover in a civil action damages, including punitive damages, as well as attorney's fees and other costs against the person or entity engaged in the violation.

The technical assistance of service providers in helping a law enforcement agency execute an electronic surveillance order is always important, and in many cases it is absolutely essential. This is increasingly the case with the advent of advanced communication services and networks such as the Internet. Title III mandates service provider assistance incidental to law enforcement's execution of electronic surveillance orders by specifying that a court order authorizing the interception of communication shall upon the request of the applicant, direct that a telecommunications "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example, in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are also subject to the electronic surveillance laws, meaning that unauthorized electronic surveillance of their customers (or anyone else) is forbidden, and criminal and civil liability may be assessed for violations. Not only are unauthorized interceptions proscribed, but so also is the use or disclosure of the contents of communications that have been illegally intercepted. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in many cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue, orders for Title III interceptions which are much more detailed than older orders which were directed against "plain old telephone services." These detailed order, in order to be successfully implemented, require more sophisticated techniques to ensure that only messages for which there is court authorization to intercept are, in fact, intercepted. The increased detail in court orders responds to two facts.

First, the complexity of modern communications networks, like the Internet, and the complexity of modern users' communications demand better discrimination than older analog communications. For example, Internet users frequently use electronic messaging services, like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call. Similarly, some Internet services, like streaming video, have more in common with broadcast media like television, than with telephone calls. These types of communications are less commonly the targets of an interception order.

Second, for many Internet services, users share communications channels, addresses, etc. These factors make the interception of messages for which law enforcement has court authorization, to the exclusion of all others, very difficult. Court orders, therefore, increasingly include detailed instructions to preclude the interception of communications that lie outside the scope of the order.

In response to a critical need for tools to implement complex court orders, the FBI developed a number of capabilities including the software program called "Carnivore." Carnivore is a very specialized network analyzer or "sniffer" which runs as an application program on a normal personal computer under the Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programmed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use Carnivore at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how Carnivore is used in practice. First, there is the issue of scale. Carnivore is a small-scale device intended for use only when and where it is needed. In fact, each Carnivore device is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.

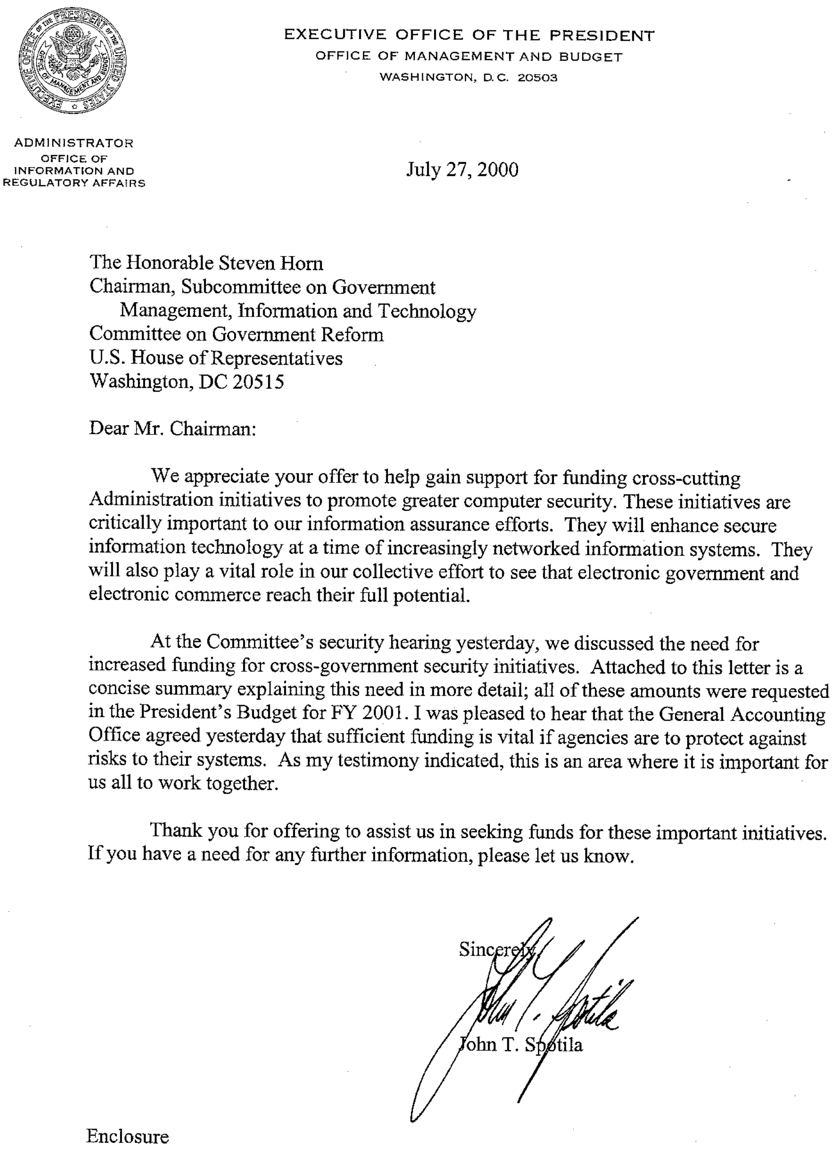
The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is connected as a passive collection device and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that our system is satisfactorily isolated from the network to which it is attached. Also, Carnivore is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This, in fact, raises the third issue - that of ISP cooperation. To date, Carnivore has, to my knowledge, never been installed onto an ISP's network without assistance from the ISP's technical personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, and I can assure you that without the technical knowledge of the ISP's personnel, it would be very difficult, and in some instances impossible, for law enforcement agencies to successfully implement, and comply with the strict language, of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using the Carnivore system is data integrity. As you know, Rule 901 of the Federal Rules of Evidence requires that authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is another key reason for preferring this system to commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I would like to say that over the last five years or more, we have witnessed a continuing steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities which have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively investigate and prevent these crimes is, in part, dependent upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so without the continued cooperation of our industry partners and innovations such as the Carnivore software. I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices, without lawful authorization from a court.

I look forward to working with the Subcommittee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank you.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

ADMINISTRATOR
OFFICE OF
INFORMATION AND
REGULATORY AFFAIRS

July 27, 2000

The Honorable Steven Horn
Chairman, Subcommittee on Government
Management, Information and Technology
Committee on Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

We appreciate your offer to help gain support for funding cross-cutting Administration initiatives to promote greater computer security. These initiatives are critically important to our information assurance efforts. They will enhance secure information technology at a time of increasingly networked information systems. They will also play a vital role in our collective effort to see that electronic government and electronic commerce reach their full potential.

At the Committee's security hearing yesterday, we discussed the need for increased funding for cross-government security initiatives. Attached to this letter is a concise summary explaining this need in more detail; all of these amounts were requested in the President's Budget for FY 2001. I was pleased to hear that the General Accounting Office agreed yesterday that sufficient funding is vital if agencies are to protect against risks to their systems. As my testimony indicated, this is an area where it is important for us all to work together.

Thank you for offering to assist us in seeking funds for these important initiatives. If you have a need for any further information, please let us know.

Sincerely,

John T. Spotila

Enclosure

FY 2001 Cross-Cutting Security Initiatives

General Services Administration

- $5.4 million to maintain the Federal Incident Response Capability (FedCIRC) the central government non-law enforcement focal point for responding to attacks, promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. A significant portion of this funding is also to continue government support of Carnegie-Mellon University's highly acclaimed Computer Emergency Response Team (CERT).

- $10 million for next generation intrusion detection. This funding would be used top establish the Federal Intrusion Detection Network (FIDNet) which would compliment FedCIRC by standardizing ongoing agency computer intrusion detection activities, automating many of the cumbersome manual processes now employed, and providing a centralized expert analytic capability that does not exist at most agencies.

Department of Commerce

- $5 million at the National Institute for Standards and Technology (NIST) to establish an expert security review team to help agencies review their systems and programs, identify unacceptable risks, and assist in mitigating them. This program is in the context of NIST's statutory responsibilities under the Computer Security Act of 1987 and Clinger-Cohen Act of 1996 to issue security guidance to the agencies.

- $6.6 million for the Critical Infrastructure Assurance Office to continue its efforts to assist government agencies in identifying and prioritizing their critical assets and interdependencies and to continue cross-sectoral public-private partnerships.

- $50 million to create the Institute for Information Infrastructure Protection at NIST. The Institute would work collaboratively with industry and academia to fill research and development gaps for key security technologies. Industry often has no incentive to invest in long-term research and development without a clear market need. Research would be performed at private corporations, universities, and non-profit research institutes.

Department of Treasury

- $7 million at Treasury to perfect the development of an interoperable government-wide infrastructure to permit authenticated electronic transactions and thus promote the electronic delivery of services to the public. In the paper-based world, government, industry, and the public rely on trusted and verifiable relationships, photo IDs, notarized signatures, and face-to-face contact to authenticate one another's identify prior to conducting business. This funding would translate those paper-based relationships into similar trusted and verifiable electronic relationships.

Office of Personnel Management and the National Science Foundation

- $7 million at the Office of Personnel Management and $11.2 million at the National Science Foundation for Federal Cyber Services/Scholarships for Service. The Scholarship for Service effort is intended to develop the next generation of Federal information technology managers by awarding scholarships for the study of information assurance and computer security in exchange for Federal Service.