Opening Statement for Subcommittee Hearing
Chairman Jon Kyl
October 6, 1999

"Critical Information Infrastructure Protection: the Threat is Real"

The Subcommittee will please come to order. Let me first welcome everyone to this hearing of the Subcommittee on Technology, Terrorism, and Government Information. At our hearing today, we will examine a growing public policy concern: the threat of hostile attack on our nation's critical information infrastructure, and the adequacy of the federal government's response to this threat. This is the fourth public hearing the Subcommittee has held on this topic in the last two years, and given the importance of the subject, it will not be our last.

The President's top advisors recently issued a report on preserving America's privacy and security in cyberspace. As the report points out, the enormous success the United States has enjoyed over the past century was due in part to the ability of our nation and its leaders to deal with the latest technological trends in a way that enhanced the security and prosperity of successive generations of Americans. At critical junctures in our history, wise government policies with regard to innovative technology have resulted in unprecedented success.

During the Industrial Age, the arrival of World War II signaled an urgent need for increased production and scientific advances. The success of America's war effort in defeating Fascism rested largely on the strength of our industrial might and the successful collaboration between our government and industry. We not only protected Americans security, but also vaulted the U.S. economy to unprecedented heights in the post-War period.

Today, the Industrial Age has become the Information Age, and computers facilitate the instant exchange of vast amounts of data and ideas. Who would have predicted just a few decades ago, that a small Defense Department research effort would result in the creation of the Internet and revolutionize our society.

As we approach the dawn of the new millennium, America again faces a

time of pivotal change. Information technology presents both an opportunity and a threat to our society, which is increasingly dependent on computers and communications equipment -- what we call our critical information infrastructure. As most Americans have learned recently, with the preparations for Y2K to make sure there are no major disruptions in services, virtually every key service is dependent on computers: from electrical power grids, to phone systems, air-traffic control, water and sewer service, medical devices, banking, and list goes on and on. Unfortunately, very few of these critical computer networks were designed with good security measures.

The changes in our society also must be viewed in context with America's changed geopolitical role in the post-Cold War world. The U.S. is the world's only superpower and our armed forces enjoy technical superiority on the battlefield. Nations and terrorist groups that are hostile to our interests, are increasingly choosing not to confront our strengths directly, that is by trying to field fleets of advanced fighter planes or ships on a par with ours, but rather are seeking to exploit our vulnerabilities, looking hard for our Achilles heel.

According to the National Security Agency, over 100 countries are working on information warfare techniques. One recent case illustrates the danger of this threat. According to *Newsweek* magazine, computer systems at the Defense and Energy Departments have been the subject of a sustained computer hacking effort from Russia. These attacks have resulted in the loss of vast quantities of data, possibly including classified naval codes and information on missile-guidance systems. These computer attacks have reportedly been very subtle. For example, the *London Sunday Times* interviewed an engineer at the Space and Naval Warfare Systems Command in San Diego, California, who described being alerted to a problem when a computer print job took an unusually long time. According to the *Times*, "To his amazement, monitoring tools showed that the file had been removed from the printing queue and transmitted to an internet server in Moscow before being sent back to San Diego."

And there are other troubling examples of computer attacks by U.S. citizens that demonstrate our weaknesses in this area. For example, one group dubbed the "Phonemasters" by the FBI manipulated computers that route telephone calls. These hackers reportedly gained access to telephone networks of companies like AT&T, British Telecom, GTE, Sprint, MCI WorldCom, and

NEWS

United States Senate
Special Committee on the Year 2000 Technology Problem

Senator Robert F. Bennett
Chairman

Senator Christopher J. Dodd
Vice-Chairman

FOR IMMEDIATE RELEASE

CONTACT: Don Meyer
(202) 224-5224

Senator Robert F. Bennett
Chairman
Senate Special Committee on the Year 2000 Technology Problem

Opening Statement at the Senate Committee on the Judiciary
Subcommittee on Technology Terrorism
and Government Information
October 6, 1999

Senator Kyl, I appreciate the outstanding work your subcommittee has done to investigate the threats to our nation's critical infrastructures. As you know, the threats from foreign-based information warfare have been increasing as rapidly as technology is developing. Threats to U.S. infrastructure are nothing new. A former KGB official just published The Sword and The Shield, a book based on secret KGB files from the 1970's detailing plans to disrupt key U.S. infrastructures. Now, the Internet has made such goals much easier to achieve – not just for the Russians but for anyone with basic skills, a little money and computer.

Information warfare is not a weapon, it is a place. A few weeks ago, I saw an early attempt to map New World. Every day, a man at Lucent tries to map the Internet. It looks nothing like the Old World. It is a tangled mass of color-coded networks. I wasn't sure if I was looking at an abstract painting. I am certain of one thing. When you begin looking at the new geography, the physical networks and teledensity blur the political and spatial world. Countries, as we know them, begin to fade and oceans disappear.

The world is not billions of years old; it is only ten years old. The globalization of the world economy and the integration of markets, nation-states, and technologies are enabling individuals, corporations, and nation-states to reach around the world farther, faster, deeper, and cheaper than ever before. While cheap global reach has tremendous benefits from a commercial perspective, it also presents unique strategic challenges to the United States.

Where is the United States if oceans disappear? Well, I can tell you where we are not. We are not sitting in the "sanctuary" of North America. We are meshed together in global infrastructures that place us within a few keystrokes of an adversary's reach. What good is a clear view of the skies and seas to the Department of Defense if an adversary chooses to travel by fiber optic cable?

-MORE-

With a few mouse clicks and a several hops through international Internet service providers, a rogue nation or well-funded, state-sponsored terrorist group could inflict serious damage on our nation's critical infrastructures, economy, and defense. They could physically attack the United States from a keyboard anywhere in the world.

If you think this can't really happen, think again. An Iranian military journal recently observed that, "[T]he Internet has been turned into a kind of weapon for warfare . . . so America's enemies are able to inflict irreparable losses on the U.S. Army through the use of the Internet." Consider this in the context that more than 120 nations have computer attack capabilities. According to Interpol, the European police agency, the Internet has some 30,000 hacker-oriented Web sites that can inflict serious damage on public or private systems; roughly 17 million people have the necessary computer skills to wreak this serious damage. The technology to cause such damage is increasingly sophisticated and the level of skill required to operate that technology is dropping rapidly.

With oceans disappearing and borders blurring, it becomes increasingly difficult to tell if an attack is international or domestic. How do you defend against a threat that is not necessarily military? What happens when you can't identify the adversary? Who responds – law enforcement or defense? What happens when civilian infrastructure and private industry are the targets? At what point does an action stop being a law enforcement issue and start being a national security threat? There are no easy answers to these questions right now.

Given the broad spectrum of methods employed in cyber attacks, and the wide range of targets, this issue transcends the narrow scope of defense, law enforcement, or intelligence. Protecting America's critical infrastructures is more than finding a balance between firewalls and firepower.

There are serious and sometimes contentious policy issues that will need to be resolved in both the legislative and executive branches. These issues will challenge the Congress to work across many different jurisdictional boundaries.

Currently, there is no common understanding of what constitutes a "nationally significant" cyber-incident. A qualitative framework must be developed that takes into account that several incidents in "seemingly" unrelated sectors may in fact be coordinated and purposeful attacks. A well-defined threshold must take into account both low-intensity incidents in multiple sectors as well as widespread disruption of a single infrastructure. Congress will need to investigate and ensure that current legislation defining the concepts of law enforcement, national security and foreign intelligence are robust enough to deal with cyber warfare, new technologies and asymmetrical threats.

Government can't solve this entire problem, but it can coordinate and facilitate reconstitution and recovery. Congress must become active and investigate ways to focus research and develop initiatives that will enable the U.S. to organize warnings, damage assessments, and coordination of cyber-reconstitution. Finally, even though oceans disappear, we need the determination and vision to ensure the integration of fundamental American ideals of liberty and justice into our national technology policy.

###

Hearing before the
Senate Judiciary Committee
Subcommittee on Technology, Terrorism and Government Information

October 6, 1999

Statement of
John S. Tritak
Director
Critical Infrastructure Assurance Office

Mr. Chairman, Madame Ranking Member, members of the Subcommittee, ladies and gentlemen, it is an honor to appear before you here today to discuss the challenges facing our Nation in the area of critical infrastructure protection. This Subcommittee has shown exceptional leadership on these issues, and I am grateful for the opportunity to work closely with you and the Congress to find ways to advance infrastructure assurance for all Americans. We all recognize that no viable solutions will be discovered or implemented without the executive and legislative branches working together for our national good.

I. Introduction

America has long depended on a complex of systems – or critical infrastructures – to assure the delivery of services vital to its national defense, economic prosperity, and social well-being. These infrastructures include telecommunications, electric power, oil and gas delivery and storage, banking and finance, transportation, and vital human and government services.

The information age has fundamentally altered the nature and extent of our dependency on these infrastructures. Increasingly, our government, economy and society are being connected together into an ever expanding and interdependent digital nervous system of computers and information systems. With this interdependence comes new vulnerabilities. One person with a computer, a modem, and a telephone line anywhere in the world can potentially break into sensitive government files, shut down an airport's air traffic control system, or cause a power outage in an entire region.

The threats posed to our critical infrastructures by hackers, terrorists, criminal organizations and foreign governments are real and growing. The nature of these threats will be addressed by Mr. Vatis of the National Infrastructure Protection Center (NIPC).

Before I discuss the initiatives the Administration is undertaking to secure our nation's critical infrastructures, I would like to discuss the historical context within which PDD-63 arose.

In the early 1990s, events such as the 1995 bombing of the Murrah Federal Building in Oklahoma City demonstrated that the federal government needed to address new types of threats and vulnerabilities – many of which the nation was unprepared to defend against.

In response to this tragedy, and other events, the Administration formed an inter-agency working group to examine the nature of the threat, our vulnerabilities, and possible long-term solutions for this aspect of our national security. The Critical Infrastructure Working Group (CIWG), chaired by then Deputy Attorney General Jamie Gorelick, and including representatives from the Defense, Intelligence, and national security communities, identified both physical and cyber threats and recommended formation of a Presidential Commission to address more thoroughly many of these growing concerns.

In July 1996, in response to the CIWG recommendation, President Clinton signed Executive Order 13010 establishing the President's Commission on Critical Infrastructure Protection (PCCIP or, the Commission). After examining infrastructure issues for over a year, the

Commission issued its report, Critical Foundations, Protecting America's Infrastructures, drawing at least four significant conclusions:

- First, critical infrastructure protection is central to our national defense, including national security and national economic power;

- Second, growing complexity and interdependence between critical infrastructures may create increased possibility that rather minor and routine disturbances can cascade into national security emergencies;

- Third, vulnerabilities are increasing steadily and the means to exploit weaknesses are readily available; practical measures and mechanisms, the commission argued, must be urgently undertaken before we are confronted with a national crisis; and

- Fourth, laying a foundation for security will depend on new forms of cooperation with the private sector, which owns and operates many of these critical infrastructure facilities.

II. PDD-63 - Overview

After releasing the PCCIP report, the Administration worked to incorporate these and other recommendations into Presidential Decision Directive 63, which was issued in May 1998. Most importantly, PDD-63 recognizes the need for a Public-Private Partnership to face these critical issues. The directive specifies sectors of the national infrastructure, primarily in the private sector, that provide critical services or functions. It designates lead agencies in the Federal Government to work as liaisons with their respective sectors to build partnerships. PDD-63 additionally recognizes that the traditional areas of national defense, foreign affairs, intelligence, and law enforcement are fundamental to infrastructure protection, are inherently the domain of the government, and stipulates that sector coordinators be designated for these areas from the associated government agencies.

PDD-63 established the position of National Coordinator for Security, Infrastructure Protection, and Counter Terrorism to orchestrate these efforts. The PDD lays out specific tasks that must be accomplished, time lines for doing so, and organizations for carrying out these missions. Key amongst them are the National Infrastructure Protection Center (NIPC), Directed by Mr. Vatis, and the National Plan Coordination Staff – now called the Critical Infrastructure Assurance Office (CIAO) – which I have the honor of directing.

PDD-63 focuses the nation's efforts on aspects of critical and immediate importance -- and I emphasize that these must be the efforts of the whole nation, for success will come only from the efforts of the private sector, state and local governments, and the Federal Government working together in an integrated and cooperative manner. Our efforts fall in three broad categories.

A. Defense and Intelligence Components

The first is the Federal Government agencies involved in defense and intelligence efforts. The armed forces and intelligence agencies have requirements and systems that are unique to their special role. This has long been recognized in law, in the way we structure these organizations, and in our national philosophy. Their efforts are, as would be expected from the sensitive and well established nature of their mission, much further along in achieving critical infrastructure protection than those of the other parts of the Federal Government. In many ways they have set the example for other agencies' efforts, and they currently share their experiences and advise on how the rest of the government might proceed. Their contribution has been very important in shaping the policy and programmatic reality the rest of the government is currently trying to establish. Mr. Richard Schaeffer, Director of the Information and Infrastructure Assurance Office for the Defense Department, has submitted a statement for the record on this and other matters, so, in cause of brevity, I will refer you to it and cover their efforts no further.

B. Government as Model

The second category of effort can be called "Government as a Model." We often say that more than 90% of our critical infrastructures are neither owned nor operated by the Federal Government. Partnerships with the private sector and State and Local Governments are therefore not just needed, but are the fundamental aspect of critical infrastructure protection. Yet, the President rightly challenged the Federal Government in PDD-63 to serve as a model for critical infrastructure protection – to put our own house in order first. As such, the Administration has focused what might appear to be a disproportionate amount of our effort early in the process on doing this by establishing a coordinated and integrated approach across the Federal Government.

- Federal Computer Security Requirements and Government Infrastructure Dependencies

One component of this effort supports aggressive, government-wide implementation of federal computer security requirements. Thus, in support of PDD-63, the President forwarded to Congress a request for a FY 2000 budget amendment that would enhance computer security and critical infrastructure protection in the Federal Government. This proposal would fund a permanent 15-member team at the Department of Commerce's National Institute of Standards and Technology (NIST) responsible for helping Agencies identify vulnerabilities, plan secure systems, and implement Critical Infrastructure Protection Plans. The budget amendment would also establish an operational fund at NIST for computer security projects among Federal Agencies, including independent vulnerability assessments, computer intrusion drills, and emergency funds to cover security fixes for systems identified to have unacceptable security risks. Among others, the Director of the team would consult with the Office of Management and Budget and the National Security Council on the team's plan to protect and enhance computer security for Federal Agencies.

Under PDD-63, the President directed the CIAO to coordinate analyses of the US Government's own dependencies on critical infrastructures. Many of the critical

infrastructures that support our nation's defense and security are shared by multiple agencies. Even within government, then, critical infrastructure outages may cascade and unduly impair delivery of critical services. The CIAO is coordinating an interagency effort to develop a more sophisticated identification of critical nodes and systems and their impact on national security government-wide. These efforts will support the work of the ERT in identifying vulnerabilities of the government's computer infrastructures, planning secure computer systems, and implementing computer security plans.

This research, when complete, will provide important information to maximize national security research and development, budgeting, and for implementing Federal computer security requirements and critical infrastructure planning within each agency.

- Federal Intrusion Detection Network (FIDNET)

PDD-63 marshals resources to improve interagency cooperation in detecting, and in responding to computer intrusions into civilian government critical infrastructure nodes. To support this effort, the Administration recently sent to Congress a FY2000 Budget Amendment to create a centralized intrusion detection and response capability in the General Services Administration (GSA). Through the use of additional staff and enhanced technology, Federal Agencies will improve upon their abilities to:

- detect computer attacks and unauthorized intrusions;
- share attack warnings and related information across agencies; and
- respond to attacks.

This amendment would provide GSA funds to pay for additional technology and personnel dedicated to intrusion detection and response. The additional personnel would improve Federal Agencies' ability to detect attacks, analyze data, and communicate attack information more swiftly, building on the existing Federal Computer Incident Response Capability (FedCIRC). The additional technology, in the form of state-of-the-art intrusion detection systems, would ensure a consistent capability in Agencies to protect critical systems.

The program -- much like a centralized burglar alarm system -- would operate within legal requirements and Government policy concerning privacy, civil liberties, and promoting confidence in users of Federal civilian computer systems. Attack and intrusion information would be gathered and analyzed by Agency experts. Only data on system anomalies would be forward to GSA for further analysis.

Neither the Federal Bureau of Investigation nor other law enforcement entities would receive information about the computer attacks and intrusions -- except under long-standing legal rules and where an Agency determines there is sufficient indication of illegal conduct. Also, private entities will not be wired to the FIDNet – no private sector entity is part of this civilian government program.

In short, FIDNet will be run by the GSA, not the FBI; will not monitor any private networks or email traffic; will confer no new authorities on any government agency; and will be fully consistent with privacy law and practice.

- Education and Training

One of the nation's important shortcomings in our efforts to protect our critical infrastructures is a shortage of skilled information technology (IT) personnel. Within the subset of information systems security personnel, the shortage is acute. Within the Federal Government, the lack of skilled information systems security personnel amounts to a crisis. This shortfall of workers reflects a scarcity of university graduate and undergraduate information security programs. In attacking this problem, we will leverage the initial efforts made by the Defense Department, National Security Agency, and some Federal Agencies.

The Federal Cyber Services (FCS) training and education initiative introduces five programs to help solve the Federal IT security personnel problem.

- *The Completion of an Office of Personnel Management IT occupational study*. This study will help identify the number of IT security positions in the Federal Government, and the training and certification requirements for these positions.

- *The development of Center(s) for Information Technology Excellence (CITE)*. These Centers will train and certify current Federal IT security personnel and maintain their skill levels throughout their careers. It will leverage the significant progress made by the Defense Department and other federal agencies on this issue.

- *The creation of a Scholarship for Service (SFS) program to recruit and educate the next generation of Federal IT security workers and managers*. This program will fund up to 300 students per year in their pursuit of undergraduate or graduate degrees in the IT security field. In return, the students will serve in the Federal IT workforce for a fixed period following graduation. The program will also have a meaningful summer work and internship element. An important part of the SFS program is the need to identify universities for participation in the program and assist in the development of IT security faculty and laboratories at these universities.

- *The development of a high school recruitment and training initiative*. This program would identify promising high school students for participation in summer work and internship programs that would lead to certification to Federal IT workforce standards and possible future employment. This effort will also examine possible programs to promote computer security awareness in secondary and high school classrooms.

- *The development and implementation of a Federal INFOSEC awareness curriculum.* This awareness effort is aimed at ensuring the entire Federal workforce is developing computer security literacy. It will leverage several outstanding existing federal agency awareness programs.

- Research and Development

A key component to our ability to protect our critical infrastructures now and in the future is a robust research and development plan. The interagency Critical Infrastructure Coordination Group (CICG) has created a process to identify technology requirements in support of the Plan. Chaired by the Office of Science and Technology Policy (OSTP), the Research and Development Sub-Group works with Agencies and the private sector to:

- gain agreement on requirements and priorities for information security research and development;
- coordinate among Federal Departments and Agencies to ensure the requirements are met within departmental research budgets and to prevent waste or duplication among departmental efforts;
- communicate with private sector and academic researchers to prevent Federally funded R&D from duplicating prior, ongoing, or planned programs in the private sector or academia; and
- identify areas where market forces are not creating sufficient or adequate research efforts in information security technology.

That process, begun in 1998, led to the Administration budget request for FY2000 of $500M for critical infrastructure protection research. Among the priorities identified by the process are:

- technology to support large-scale networks of intrusion detection monitors;
- artificial intelligence and other methods to identify malicious code (trap doors) in operating system code;
- methodologies to contain, stop, or eject intruders, and to mitigate damage or restore information-processing services in the event of an attack or disaster;
- technologies to increase network reliability, system survivability, and the robustness of critical infrastructure components and systems, as well as the critical infrastructures themselves; and
- technologies to model infrastructure responses to attacks or failures; identify interdependencies and their implications; and locate key vulnerable nodes, components, or systems.

C. Public-Private Partnership

Thirdly, and as discussed above, one of the most important components of PDD-63

implementation is the development of collaborative partnerships among and between the private sector, state and local governments, and the Federal Government. The importance of this effort cannot be overstated and is made clear by considering just a few scenarios. If the natural gas delivery system you rely on for heat and cooking fails in January due to an attack on the computer systems that direct its operations, you will take small comfort in fact that the Federal Government has a critical infrastructure protection plan in place. In fact, all our efforts to put the Federal Government's house in order and to serve as a model for industry will be of little service if our government information systems are impossible to break into, but the electrical power that they operate on is shut down by malicious actions of a foreign government. The list of examples goes on and on, and none of these systems is owned or operated by the Federal Government.

These vignettes put the situation in perspective – we are faced with a fascinating and challenging problem. This is the first time I am aware of in our national history that by creating policy and expending resources, the Federal Government cannot alone solve a national security problem. So what are we doing about it? If by "we" you understand "the government" then the answer must necessarily be unsatisfactory – because the government alone cannot protect the nation's infrastructures. But if by "we" you understand "the nation" – the Federal Government in a coordinated and integrated effort with state and local government, industry, academia and other concerned groups – then I am happy to report that we have made a good beginning, and are developing a strong future.

Just last Friday, Treasury Secretary Summers announced the formation of the Financial Sector Information Sharing and Analysis Center – "ISAC" for short. ISACs are private sector owned and operated entities that serve as focal points for their associated sector of the economy. Because they are defined individually by their member organizations, they will not all be identical. They are, however, all to be the coordinating and analyzing body for cyber attacks on their specific sector. I want to emphasize that these ISACs are neither set up, nor supervised by the Federal Government, although the Federal Government will assist these critical sectors in setting up their ISAC, through the Sector Liaisons, if asked. The government will share what information we can on cyber attacks with the ISACs to help them protect their sector, and we will encourage them to share appropriately sanitized information with us to help us protect government agencies and functions. But this sharing from ISACs to government will be on an entirely voluntary basis, both in amount of information and the level of detail. No requirement exists or will exist that mandates information sharing.

While these ISACs, would work within the sectors of the economy that own and operate critical infrastructure, as stipulated in PDD-63, this is not intended to be limiting. Other sectors or groupings within industry could establish ISACs, and we would assist them in this. Furthermore, practically every aspect of our nation relies on critical infrastructures. This makes CIP a fundamentally important issue for not just those companies that own and operate critical infrastructure, but also for those that rely on it to do business. They can and must have a voice in this public/private partnership.

Recently, the President issued an Executive Order establishing a National Infrastructure Assurance Council (NIAC). This Presidential advisory body will be comprised of leaders

from the Private Sector, State and Local governments, and the Federal Government. It will examine key aspects of critical infrastructure assurance, and report to the President.

The final indispensable members of this partnership are state and local governments. They have the fundamentally important roles of providing and regulating many if not most essential services. They are the front line forces in the event of disasters or attacks on infrastructures. Some have moved quite far in their critical infrastructure protection efforts – New Mexico, for example, under the direction of Dr. Dan O'Neil, has a very strong and growing critical infrastructure protection partnership with key private sector entities. Furthermore, we have long had strong relationships with state and local governments on specific issues related to critical infrastructure protection, such as state and local emergency management organizations with FEMA, and state and local law enforcement agencies through the FBI and others national law enforcement agencies. This area is one in which much work remains to be done, and I look forward to working with each Congressional Delegation as we define the issues and solutions.

III. Conclusion

In conclusion, much has been done since PDD-63 was issued in 1998. My staff and I are committed to building on this promising beginning, coordinating the government's efforts into an integrated holistic program for critical infrastructure protection under the direction of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. We have much work left to do, and I look forward to with the members of this committee, indeed with the Congress as a whole, as we wrestle with this developing field and implement solutions. I look forward to your questions.

Statement for the Record
Michael A. Vatis
Director, National Infrastructure Protection Center
Federal Bureau of Investigation
before the
Senate Judiciary Committee
Subcommittee on Technology and Terrorism
Washington, D. C.
October 6, 1999

Introduction

Mr. Chairman, Senator Feinstein, and Members of the Committee: Thank you for inviting me here today to discuss critical infrastructure protection issues. Mr. Chairman, you and this committee have been leaders in recognizing the importance of these issues and the urgency of addressing the new threats to our national security in the Information Age, and I welcome this opportunity to share our perspectives with you today. As you know, the Federal Government is developing its capabilities for dealing with threats to our nation's infrastructures. Presidential Decision Directive-63 set in motion an unprecedented effort to protect our nation's critical infrastructures, which the PDD defined as "those physical and cyber-based systems essential to the minimum operations of the economy and government." Critical infrastructures include telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both public and private. The PDD formally designated the National Infrastructure Protection Center (NIPC) to have a central operational role in the government's effort. The Center works closely with the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism; the Department of Defense (DoD); the U.S. Intelligence Community (USIC); other federal agencies; and the private sector to protect our critical infrastructures. My statement will cover the spectrum of threats we are facing and the status of the NIPC and its activities.

Spectrum of Threats

The news media is filled with examples of intrusions into government and private sector computer networks. Politically motivated hackers have been attacking numerous U.S. Government websites, including the Senate's. Deputy Secretary of Defense John Hamre reported in February that DoD is "detecting 80 to 100 [potential hacking] events daily." We have had several damaging computer viruses this year, including the Melissa Macro Virus, the Explore.Zip Worm, and the CIH (Chernobyl) Virus. Computer Economics, Inc., a California firm, estimates that damage in the first two

quarters of 1999 from viruses has topped $7 billion. The FBI's case load for computer hacking and network intrusion cases has doubled each of the last two years. Currently we have over 800 pending investigations. In its 1999 survey, the Computer Security Institute estimated the total financial losses by the 163 businesses it surveyed from computer security breaches at $123.7 million. This includes everything from theft of proprietary data to denial of service on networks. E-commerce has become so important that firms, including Sedgwick Group PLC (in cooperation with IBM), Lloyds of London, and Network Risk Management Services, are now offering "hacker insurance."

Sensitive Intrusions

In the past few years we have seen a series of intrusions into numerous Department of Defense computer networks as well as networks of other federal agencies, universities, and private sector entities. Intruders have successfully accessed U.S. Government networks and took large amounts of unclassified but sensitive information. In investigating these cases, the NIPC has been coordinating with FBI Field Offices, the Department of Defense, and other government agencies, as circumstances require. But it is important that the Congress and the American public understand the very real threat that we are facing in the cyber realm, not just in the future, but now.

Information Warfare

Perhaps the greatest potential threat to our national security is the prospect of "information warfare" by foreign militaries against our critical infrastructures. We know that several foreign nations are already developing information warfare doctrine, programs, and capabilities for use against each other and the United States or other nations. Foreign nations are developing information warfare programs because they see that they cannot defeat the United States in a head-to-head military encounter and they believe that information operations are a way to strike at what they perceive as America's Achilles Heel -- our reliance on information technology to control critical government and private sector systems. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. In addition, during the recent conflict in Yugoslavia, hackers sympathetic to Serbia electronically "ping" attacked NATO web servers. And Russian as well as other individuals supporting the Serbs attacked websites in NATO countries, including the United States, using virus-infected e-mail and hacking attempts. Over 100 entities in the United States received these e-mails. Several British organizations lost files and databases. These attacks did not cause any disruption of the military effort, and the attacked entities quickly recovered. But such attacks are portents of much more serious attacks that we can expect foreign adversaries to attempt in future conflicts.

Foreign intelligence services

Foreign intelligence services have adapted to using cyber tools as part of their information gathering and espionage tradecraft. In a case dubbed "the Cuckoo's Egg," between 1986 and 1989 a ring of West German hackers penetrated numerous military, scientific, and industry computers in the United States, Western Europe, and Japan, stealing passwords, programs, and other information which they sold to the Soviet KGB. Significantly, this was over a decade ago -- ancient history in Internet years. While I cannot go into specifics about the situation today in an open hearing, it is clear that foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. government and private sector information.

Terrorists

Terrorists are known to use information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely. For example, convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his laptop computer. Moreover, some groups have already used cyber attacks to inflict damage on their enemies' information systems. For example, a group calling itself the Internet Black Tigers conducted a successful "denial of service" attack on servers of Sri Lankan government embassies. Italian sympathizers of the Mexican Zapatista rebels attacked web pages of Mexican financial institutions. And a Canadian government report indicates that the Irish Republican Army has considered the use of information operations against British interests. We are also concerned that Aum Shinrikyo, which launched the deadly Sarin gas attack in the Tokyo subway system, could use its growing expertise in computer manufacturing and Internet technology to develop "cyber terrorism" weapons for use against Japanese and U.S. interests. Thus while we have yet to see a significant instance of "cyber terrorism" with widespread disruption of critical infrastructures, all of these facts portend the use of cyber attacks by terrorists to cause pain to targeted governments or civilian populations by disrupting critical systems.

Criminal Groups

We are also beginning to see the increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain. For example, in 1994 the U.S. Secret Service uncovered a $50 million phone card scam that abused the accounts of AT&T, MCI, and Sprint customers. In addition, in 1994-95 an organized crime group headquartered in St. Petersburg, Russia, transferred $10.4 million from Citibank into accounts all over the world. After surveillance and investigation by the FBI's New York field office, all but $400,000 of the funds were recovered. In another case, Carlos Felipe Salgado, Jr. gained unauthorized access to several Internet Service

Providers in California and stole 100,000 credit card numbers with a combined limit of over $1 billion. The FBI arrested him in the San Francisco International Airport when he tried to sell the credit card numbers to a cooperating witness for $260,000. With the expansion of electronic commerce, we expect to see an increase in hacking by organized crime as the new frontier for large-scale theft.

Just two weeks ago, two members of a group dubbed the "Phonemasters" were sentenced after their conviction for theft and possession of unauthorized access devices (18 USC §1029) and unauthorized access to a federal interest computer (18 USC §1030). The "Phonemasters" are an international group of criminals who penetrated the computer systems of MCI, Sprint, AT&T, Equifax, and even the FBI's National Crime Information Center (NCIC). Under judicially approved electronic surveillance orders, the FBI's Dallas Field Office made use of new data intercept technology to monitor the calling activity and modem pulses of one of the suspects, Calvin Cantrell. Mr. Cantrell downloaded thousands of Sprint calling card numbers, which he sold to a Canadian individual, who passed them on to someone in Ohio. These numbers made their way to an individual in Switzerland and eventually ended up in the hands of organized crime groups in Italy. Mr. Cantrell was sentenced to two years as a result of his guilty plea, while one of his associates, Cory Lindsay, was sentenced to 41 months.

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

Virus Writers

Virus writers are posing an increasingly serious threat to networks and systems worldwide. As noted above, we have had several damaging computer viruses this year, including the Melissa Macro Virus, the Explore.Zip worm, and the CIH (Chernobyl) Virus. The NIPC frequently sends out warnings regarding particularly dangerous viruses.

Earlier this year, we reacted quickly to the spread of the Melissa Macro Virus. While there are dozens of viruses released every day, the speedy propagation of Melissa and its effects on networks caused us great concern. Within hours of learning about the virus on Friday, March 26, 1999, we had coordinated with key cyber response components of DoD and the Computer Emergency Response Team (CERT) at Carnegie-Mellon University. Our Watch operation went into 24-hour posture and sent out warning messages to federal agencies, state and local law enforcement, FBI Field Offices, and

the private sector. Because the virus affected systems throughout the public, we also took the unusual step of issuing a public warning through the FBI's Public Affairs Office and on our website. These steps helped mitigate the damage by alerting computer users of the virus and of protective steps they could take.

On the investigative side, the NIPC acted as a central point of contact for the Field Offices who worked leads on the case. A tip received by the New Jersey State Police from America Online, and their follow-up investigation with the FBI's Newark Field Office, led to the April 1, 1999 arrest of David L. Smith. Search warrants were executed in New Jersey by the New Jersey State Police and FBI Special Agents from the Newark Field Office.

Just in the last few weeks we have seen reports on the Suppl Word Macro virus, the toadie.exe virus, and the W97M/Thurs.A (or Thursday) virus. This last virus has already infected over 5,000 machines, according to news reports, and deletes files on victim's hard drives. The payload of the virus is triggered on 12-13 and disables the macro virus protection in Word 97. We are also concerned with the propagation of a Trojan Horse called Back Orifice 2000, which allows malicious actors to monitor or tamper with computers undetected by the users.

Virus writers are not often broken out as a threat category, and yet they often do more damage to networks than hackers do. The prevalence of computer viruses reminds us that we all have to be very careful about the attachments we open and we all must be sure to keep our anti-virus software up-to-date.

Hactivism

Recently we have seen a rise in what has been dubbed "hacktivism"-- politically motivated attacks on publicly accessible web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into web sites to send a political message. While these attacks generally have not altered operating systems or networks, they still damage services and deny the public access to websites containing valuable information and infringe on others' right to communicate. One such group is called the "Electronic Disturbance Theater," which promotes civil disobedience on-line in support of its political agenda regarding the Zapatista movement in Mexico and other issues. This past spring they called for worldwide electronic civil disobedience and have taken what they term "protest actions" against White House and Department of Defense servers. Supporters of Kevin Mitnick, recently convicted of numerous computer security offenses, hacked into the Senate webpage and defaced it in May and June of this past year. The Internet has enabled new forms of political gathering and information sharing for those who want to advance social causes; that is good for our democracy. But illegal activities that disrupt e-mail servers, deface web-sites, and prevent the public from accessing

information on U.S. government and private sector web sites should be regarded as criminal acts that deny others their First Amendment rights to communicate rather than as an acceptable form of protest.

"Recreational" Hackers

Virtually every day we see a report about "recreational hackers," or "crackers," who crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, the recreational hacker can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use.

These types of hacks are very numerous and may appear on their face to be benign. But they can have serious consequences. A well-known example of this involved a juvenile who hacked into the NYNEX (now Bell Atlantic) telephone system that serviced the Worcester, Massachusetts area using his personal computer and modem. The hacker shut down telephone service to 600 customers in the local community. The resulting disruption affected all local police and fire 911 services as well as the ability of incoming aircraft to activate the runway lights at the Worcester airport. Telephone service was out at the airport tower for six hours. The U.S. Secret Service investigation of this case also brought to light a vulnerability in 22,000 telephone switches nationwide that could be taken down with four keystrokes. Because he was a juvenile, however, the hacker was sentenced to only two years probation and 250 hours of community service, and was forced to forfeit the computer equipment used to hack into the phone system and reimburse the phone company for $5,000. This case demonstrated that an attack against our critical communications hubs can have cascading effects on several infrastructures. In this case, transportation, emergency services, and telecommunications were disrupted. It also showed that widespread disruption could be caused by a single person from his or her home computer.

Insider Threat

The disgruntled insider is a principal source of computer crimes. Insiders do not need a great deal of knowledge about computer intrusions, because their knowledge of victim systems often allows them to gain unrestricted access to cause damage to the system or to steal system data. The 1999 Computer Security Institute/FBI report notes that 55% of respondents reported malicious activity by insiders.

There are many cases in the public domain involving disgruntled insiders. For example, Shakuntla Devi Singla used her insider knowledge and another employee's password and logon identification to delete data from a U.S. Coast Guard personnel database system. It took 115 agency

employees over 1800 hours to recover and reenter the lost data. Ms. Singla was convicted and sentenced to five months in prison, five months home detention, and ordered to pay $35,000 in restitution.

In another case, a former Forbes employee named George Parente hacked got into Forbes systems using another employee's password and login identification and crashed over half of Forbes' computer network servers and erased all of the data on each of the crashed services. The data could not be restored. The losses to Forbes were reportedly over $100,000.

Identifying the Intruder

One major difficulty that distinguishes cyber threats from physical threats is determining who is attacking your system, why, how, and from where. This difficulty stems from the ease with which individuals can hide or disguise their tracks by manipulating logs and directing their attacks through networks in many countries before hitting their ultimate target. The now well know "Solar Sunrise" case illustrates this point. Solar Sunrise was a multi-agency investigation (which occurred while the NIPC was being established) of intrusions into more than 500 military, civilian government, and private sector computer systems in the United States, during February and March 1998. The intrusions occurred during the build-up of United States military personnel in the Persian Gulf in response to tension 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. Agencies involved in the investigation included the FBI, DoD, NASA, Defense Information Systems Agency, AFOSI, and the Department of Justice.

The timing of the intrusions and links to some Internet Service Providers in the Gulf region caused many to believe that Iraq was behind the intrusions. The investigation, however, revealed that two juveniles in Cloverdale, California and several individuals in Israel were the culprits. Solar Sunrise thus demonstrated to the interagency community how difficult it is to identify an intruder until facts are gathered in an investigation, and why assumptions cannot be made until sufficient facts are available. It also vividly demonstrated the vulnerabilities that exist in our networks; if these individuals were able to assume "root access" to DoD systems, it is not difficult to imagine what hostile adversaries with greater skills and resources would be able to do. Finally, Solar Sunrise demonstrated the need for interagency coordination by the NIPC.

Special Threat: Y2K Malicious Activity

The main concern with the Y2K rollover is, of course, the possibility of widespread service

outages caused by the millennium date problem in older computer systems. The President's Y2K Council has done an excellent job in helping the nation prepare for the rollover event. Given our overall mission under PDD 63, the NIPC's role with regard to Y2K will be to maintain real-time awareness of *intentional* cyber threats or incidents that might take place around the transition to 2000, disseminate warnings to the appropriate government and private sector parties, and coordinate the government's response to such incidents. We are not responsible for dealing with system outages caused by the millennium bug. Because of the possibility that there might be an increase in malicious activity around January 1, 2000, we have formulated contingency plans both for NIPC Headquarters and the FBI Field Offices.

We are presently augmenting our existing relationships and information-sharing mechanisms with relevant entities in the federal government, such as the Information Coordination Center (ICC), state and local governments, private industry, and the CERT/FIRST community. Information will come to us from a variety of places, including FBI field offices and Legal Attaches overseas, as well as the ICC. FBI field offices are also tasked to establish Y2K plans for their regions of responsibility. In essence, all of the activities that we will undertake during the rollover period are ones we perform everyday. The difference is that we will be prepared to conduct them at an increased tempo to deal with any incidents occurring during the Y2K rollover.

There is one potential problem associated with Y2K that causes us special concern -- the possibility that malicious actors, foreign or domestic, could use the Y2K remediation process to install malicious code in the "remediated" software. Thousands of companies across the United States and around the world are busy having their source code reviewed to ensure that they are "Y2K compliant." Those who are doing the Y2K remediation are almost always contractors who are given the status of a trusted insider with broad authority to review and make changes to the source code that runs information systems. These contractors could, undetected, do any of the following to compromise systems:

- Install Trap Doors: By installing trap doors, intruders can later gain access to a system through an opening that they have created and then exploit or attack the system;

- Obtain "Root Access": Given their level of access, remediation companies can gain the same extensive privileges as the system administrator, allowing them to steal or alter information or engage in a "denial of service" attack on the system.

- Implant Malicious Code: By implanting malicious code, someone could place a logic bomb or a time-delayed virus in a system that will later disrupt it. A malicious actor could also implant a program to compromise passwords or other aspects of system security.

- Map Systems. By mapping systems as a trusted insider, a contractor can gain valuable information to sell to economic competitors or even foreign intelligence agencies.

Systems can be compromised for any number of purposes, including foreign intelligence activities, information warfare, industrial espionage, terrorism, or organized crime. And since any vulnerabilities that are implanted will persist as long as the software is in place, this is a problem that will last well beyond January 1, 2000. Companies and government agencies therefore need to determine how they will deal with this potential "Post-Y2K problem" on their critical systems.

We have little concrete evidence so far of vendors' planting malicious code during remediation. But the threat is such that companies should take every precaution possible. Of course, checking the remediation work to make sure that no malicious code was implanted in a system is no easy matter. If reviewing the millions of lines of code at issue were simple, there would be little need for Y2K contractors in the first place. Nevertheless, given the vulnerabilities that could be implanted in critical systems, it is imperative that the client companies do as much as possible to check the background of the companies doing their remediation work, oversee the remediation process closely, and review new code as closely as possible and remove any extraneous code. Further, companies should test for trap doors and other known vulnerabilities to cracking. Companies can also use "red teams" to try to crack the software and further determine if trap doors exist.

Status of the NIPC

The NIPC is an interagency Center located at the FBI. Created in 1998, the NIPC serves as the focal point for the government's efforts to warn of and respond to cyber intrusions. In PDD-63, the President directed that the NIPC "serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity." The PDD further states that the mission of the NIPC "will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response."

Thus, 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 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 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 grids, 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. Under this program, managed by the NIPC at FBIHQ, "NIPCI" squads consisting of at least seven agents have been created in 10 Field Offices: Washington D.C., New York, San Francisco, Chicago, Dallas, Los Angeles, Atlanta, Charlotte, Boston, and Seattle. For FY 2000, we intend to reallocate our existing field agent compliment to create six additional squads in Baltimore, Houston, Miami, Newark, New Orleans, and San Diego. Because of resource constraints, the other field offices have only 1 - 5 agents dedicated to working NIPCIP matters.

The NIPC's mission clearly requires the involvement and expertise of many agencies other than the FBI. This is why the NIPC, though housed at the FBI, is an interagency center that brings together personnel from all the relevant agencies. In addition to our 79 FBI employees, the NIPC currently has 28 representatives from: DoD (including the military services and component agencies), the CIA, DOE, NASA, the State Department as well as federal law enforcement, including the U.S. Secret Service, the U.S. Postal Service and, until recently, the Oregon State Police. The NIPC is in the process of seeking additional representatives from State and local law enforcement.

But clearly we cannot rely on government personnel alone. Much of the technical expertise needed for our mission resides in the private sector. Accordingly, we rely on contractors to provide technical and other assistance. We are also in the process of arranging for private sector

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 increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators."

In order to perform its role, the NIPC is continuing to establish a network of relationships with a wide range of entities in both the government and the private sector. The PDD provides for this in several ways. First, it states that the Center will "include representatives from the FBI, U.S. Secret Service, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, Intelligence Community and Lead Agencies."[1] 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 timely 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." By bringing other agencies directly into the Center and building direct communication linkages, the Center provides a means of coordinating the government's cyber expertise and ensuring full sharing of information, consistent with applicable laws and regulations.

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 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.

---

[1] The Lead Agencies are: Commerce for information and communications; 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 is performing the lead agency and special functions roles specified for "Justice/FBI" in the PDD.

representatives to serve in the Center full time. In particular, the Attorney General and the Information Technology Association of America (ITAA) announced in April that the ITAA would detail personnel to the NIPC as part of a "Cybercitizens Partnership" between the government and the information technology (IT) industry. Information technology industry representatives serving in the NIPC would enhance our technical expertise and our understanding of the information and communications infrastructure.

NIPC Activities

The NIPC's operations can be divided into three categories: protection, detection, and response.

Protection:

Our role in protecting infrastructures against cyber intrusions is not to advise the private sector on what hardware or software to use or to act as their systems administrator. Rather, our role is to provide information about threats, ongoing incidents, and exploited vulnerabilities so that government and private sector system administrators can take the appropriate protective measures. The NIPC is developing a variety of products to inform the private sector and other government agencies of threats, including: warnings, alerts, and advisories; the Infrastructure Protection Digest; Critical Infrastructure Developments; CyberNotes; and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law and the need to protect intelligence sources and methods, and law enforcement investigations. For example, the Infrastructure Protection Digest is a quarterly publication providing analyses and information on critical infrastructure issues. The Digest provides analytical insights into major trends and events affecting the nation's critical infrastructures. It is usually published in both classified and unclassified formats and reaches national security and civilian government agency officials as well as infrastructure owners. Critical Infrastructure Developments is distributed bi-weekly to private sector entities. It contains analyses of recent trends, incidents, or events concerning critical infrastructure protection. CyberNotes is another NIPC publication designed to provide security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and critical infrastructure-related best practices. It is published twice a month on our website and disseminated in hard copy to government and private sector audiences.

The NIPC, in conjunction with the private sector, has also developed an initiative called "InfraGard" to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions and exploited vulnerabilities, with the goal of increasing protection of critical infrastructures. The initiative encourages the exchange of information by

government and private sector members through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. The initiative includes an intrusion alert network using encrypted e-mail, a secure website and local chapter activities. A critical component of InfraGard is the ability of industry to provide information on intrusions to the NIPC and the local FBI Field Office using secure communications in both a detailed and a "sanitized" format. The local FBI Field Offices can, if appropriate, use the detailed version to initiate an investigation, while the NIPC can analyze that information in conjunction with law enforcement, intelligence, open source, or other industry information to determine if the intrusion is part of a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. InfraGard also provides us with a regular, secure method of providing additional security related to information to the private sector based on information we obtained from law enforcement investigations and other sources. InfraGard has recently been expanded to a total of 21 FBI Field Offices. The program will be expanded to the rest of the country later this year.

Under PDD-63, the NIPC also serves as the U.S. government's "Lead Agency" for the Emergency Law Enforcement Services Sector. As Sector Liaison for law enforcement, the NIPC and a "Sector Coordinator" committee representing state and local law enforcement are formulating a plan to reduce the vulnerabilities of state and local law enforcement to cyber attack and are developing methods and procedures to share information within the sector. The NIPC and the FBI Field Offices are also working with the State and local law enforcement agencies to raise awareness with regard to vulnerabilities in this sector.

Detection:

Given the ubiquitous vulnerabilities in existing Commercial Off-the-Shelf (COTS) software, intrusions into critical systems are inevitable for the foreseeable future. Thus, detection of these intrusions is critical if the U.S. Government and critical infrastructure owners and operators are going to be able to respond. To improve our detection capabilities, we first need to ensure that we are fully collecting, sharing, and analyzing all extant information from all relevant sources. It is often the case that intrusions can be discerned simply by collecting bits of information from various sources; conversely, if we don't collate these pieces of information for analysis, we might not detect the intrusions at all. Thus the NIPC's role in collecting information from all sources and performing analysis in itself aids the role of detection.

The NIPC is currently concentrating on developing and implementing reliable mechanisms for receiving, processing, analyzing and storing information provided by government and private sector entities. This information is being used by NIPC analysts to develop tactical and strategic warning

indicators of cyber threats and attacks. The NIPC and North American Energy Reliability Council (NERC) have established an industry-based Electric Power Working Group to develop tactical warning indicators and information sharing procedures for the electric power sector. The NIPC also has developed mechanisms to share cyber incident information with both government agencies and private companies in the telecommunications sector. In the long-term, our indications and warning efforts will require participation by the Intelligence Community, DoD, the sector lead agencies, other government agencies, federal, State and local law enforcement, and the private sector owners and operators of the infrastructures.

Another initiative that will aid in the detection of network intrusions is the "Federal Intrusion Detection Network" ("FIDNet"), a National Security Council initiative that would be managed by the General Services Administration. Many agencies already have their own intrusion detection systems. FIDNet will enhance agencies' cyber security by linking their intrusion detection systems together so that suspicious patterns of activity can be detected and alerts issued across agencies. The goal of FIDNet is to detect intrusions in the federal civilian agencies' critical computer systems. (Contrary to recent press reports, FIDNet will not extend to private sector systems.) To do this, critical network event data will be captured and analyzed so that patterns can be established and, in the event of an attack, warnings issued. FIDNet will be the civilian agency counterpart for the automated detection system currently deployed across Department of Defense systems. FIDNet, under current plans, will consist of the following: sensors at key network nodes; a centrally managed GSA facility, the Federal Intrusion Detection Analysis Center (FIDAC), to analyze the technical data from the nodes; and secure storage and dissemination of collected information. The NIPC will receive reports from the FIDAC when there is evidence of a possible federal crime (such as a violation of 18 U.S.C §1030). Using all-source information, the Center would then analyze intrusions and other significant incidents to implement response efforts and support and inform national security decision-makers. FIDNet-derived information would also be combined with all-source reporting available to the NIPC to produce analysis and warning products which will be distributed to government, private sector companies, and the public, as appropriate.

Response:

The NIPC's and the FBI's role in response principally consists of investigating intrusions to identify the responsible party and issuing warnings to affected entities so that they can take appropriate protective steps. As discussed earlier, in the cyber world, determining what is happening during a suspected intrusion is difficult, particularly in the early stages. An incident could be a system probe to find vulnerabilities or entry points, an intrusion to steal or alter data or plant sniffers or malicious code, or an attack to disrupt or deny service. The cyber crime scene is totally different from a crime scene in the physical world in that it is dynamic -- it grows, contracts, and can change shape. Determining

whether an intrusion is even occurring can often be difficult in the cyber world, and usually a determination cannot be made until after an investigation is initiated. In the physical world, by contrast, one can see instantly if a building has been bombed or an airliner brought down.

Further, the tools used to perpetrate a cyber terrorist attack can be the same ones used for other cyber intrusions (simple hacking, foreign intelligence gathering, organized crime activity to steal data, etc.), making identification and attribution more difficult. The perpetrators could be teenagers, criminal hackers, electronic protestors, terrorists, foreign intelligence services, or foreign military. In order to attribute an attack, FBI Field Offices can gather information from within the United Sates using either criminal investigative or foreign counter-intelligence authorities, depending on the circumstances. This information is necessary not only to identify the perpetrator but also to determine the size and nature of the intrusion: how many systems are affected, what techniques are being used, and what the purpose of the intrusions is--disruption, espionage, theft of money, etc.

Relevant information also could come from the U.S. Intelligence Community (if the attack is from a foreign source), other U.S. government agency information, state and local law enforcement, private sector contacts, the media, other open sources, or foreign law enforcement contacts. The NIPC's role is to coordinate and collect this information.

On the warning side, if we determine an intrusion is imminent or underway, the Watch and Warning Unit is responsible for formulating warnings, alerts, or advisories and quickly disseminating them to all appropriate parties. If we determine an attack is underway, we can issue warnings using an array of mechanisms, and send out sanitized and unsanitized warnings to the appropriate parties in the government and the private sector so they can take immediate protective steps. The Center has issued 22 warnings, alerts, or advisories between January 4 and September 22, 1999.

Two other NIPC initiatives are directed to improving our response capabilities. First, to respond appropriately, our field investigators need the proper training. Training FBI and other agencies' investigators is critical if we hope to keep pace with the rapidly changing technology and be able to respond quickly and effectively to computer intrusions. The NIPC has been very active in training. These training efforts will help keep us at the cutting edge of law enforcement and national security in the 21st Century. The Center provided training to 314 attendees in FY 1998. In FY 99, over 383 FBI Agents, state and local law enforcement representatives, and representatives from other government agencies have taken FBI-sponsored courses on computer intrusions and network analysis, the workings of the energy and telecommunications key assets, and other relevant topics.

Second, our Key Asset Initiative (KAI) facilitates response to threats and intrusion incidents by building liaison and communication links with the owners and operators of individual companies in the

critical infrastructure sectors and enabling contingency planning. The KAI began in the 1980s and focused on physical vulnerabilities to terrorism. Under the NIPC, the KAI has been reinvigorated and expanded to focus on cyber vulnerabilities as well. The KAI initially will involve determining which assets are key within the jurisdiction of each FBI Field Office and obtaining 24-hour points of contact at each asset in cases of emergency. Eventually, if future resources permit, the initiative will include the development of contingency plans to respond to attacks on each asset, exercises to test response plans, and modeling to determine the effects of an attack on particular assets. FBI Field Offices will be responsible for developing a list of the assets within their respective jurisdictions, while the NIPC will maintain the national database. The KAI is being developed in coordination with DOD and other agencies.

Conclusion

While the NIPC has accomplished much over the last year in building the first national-level operational capability to respond to cyber intrusions, much work remains. We have learned from cases that successful network investigation is highly dependent on expert investigators and analysts, with state of the art equipment and training. We have begun to build that capability both in the FBI Field Offices and at NIPC Headquarters, but we have much work ahead if we are to build our resources and capability to keep pace with the changing technology and growing threat environment and be capable of responding to several major incidents at once.

We have also demonstrated how much can be accomplished when agencies work together, share information, and coordinate their activities as much as legally permissible. But on this score, too, more can be done to achieve the interagency and public-private partnerships called for by PDD-63. We need to ensure that all relevant agencies are sharing information about threats and incidents with the NIPC and devoting personnel and other resources to the Center so that we can continue to build a truly interagency, "national" center. Finally, we must work with Congress to make sure that policy makers understand the threats we face in the Information Age and what measures are necessary to secure our Nation against them. I look forward to working with the Members and Staff of this Committee to address these vitally important issues.

Thank you.

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at 10:00 am
Wednesday
October 6, 1999

CRITICAL INFRASTRUCTURE PROTECTION

Fundamental Improvements Needed to Assure Security of Federal Operations

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

GAO
Accountability * Integrity * Reliability

GAO/T-AIMD-00-7

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss the "cyber," or computer security aspects of critical infrastructure protection. Since the early 1990s, an explosion 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 including telecommunications, power distribution, emergency services, law enforcement, national defense, and other government services.

Today, I will focus on federal agency performance in addressing computer security issues. Recent audits by GAO and agency inspectors general (IG) show that our government is not adequately protecting critical federal operations and assets from computer-based attacks. These audits show that 22 of the largest federal agencies have significant computer security weaknesses. Addressing this widespread and persistent problem requires significant management attention and action within individual agencies as well as increased coordination and oversight at the governmentwide level. I will now provide greater detail on these problems and discuss broader issues that need to be considered as a national strategy for critical infrastructure protection is being considered.

WEAK CONTROLS PLACE FEDERAL PROGRAMS AT RISK

GAO and IG reports issued over the last 5 years describe persistent computer security weaknesses that place federal operations such as national defense, law enforcement, air traffic control, and benefit payments at risk of disruption, as well as fraud and inappropriate

disclosures.[1] Our most recent analysis, of reports issued during fiscal year 1999, identified significant computer security weaknesses in 22 of the largest federal agencies.[2] These included weaknesses in (1) controls over access to sensitive systems and data, (2) controls over software development and changes, and (3) continuity of service plans. These types of weaknesses increase the risk that intruders or authorized users with malicious intentions could read, modify, delete, or otherwise damage information or disrupt operations for purposes, such as fraud, sabotage, or espionage. This body of audit evidence led us, in February 1997 and again in January 1999, to designate information security as a governmentwide high-risk area in reports to the Congress.[3]

Examples of these weaknesses and the risks they present include the following.

- In May 1999, we reported that, as part of our tests of the National Aeronautics and Space Administration's (NASA) computer-based controls, we successfully penetrated several mission-critical systems. Having obtained access, we could have disrupted NASA's ongoing command and control operations and stolen, modified, or destroyed system software and data.[4]

- In August 1999, we reported that serious weaknesses in Department of Defense (DOD) information security continue to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data. These weaknesses impair DOD's ability to (1) control physical and electronic access to its systems and data, (2) ensure that software running on its systems is

[1] Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996), Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 23, 1998).

[2] Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences (GAO/AIMD-00-01, October 1, 1999).

[3] High Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997) and High Risk Series: An Update (GAO/HR-99-1, January 1999).

[4] Information Security: Many NASA Mission-Critical Systems Face Serious Risks (GAO/AIMD-99-47, May 20, 1999).

properly authorized, tested, and functioning as intended, (3) limit employees' ability to perform incompatible functions, and (4) resume operations in the event of a disaster. As a result, numerous Defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll, have already been adversely affected by system attacks or fraud.[5]

- In July 1999, we reported that the Department of Agriculture's (USDA) National Finance Center (NFC) had serious access control weaknesses that affected its ability to prevent and/or detect unauthorized changes to payroll and other payment data or computer software. NFC develops and operates administrative and financial systems, including payroll/personnel, property management, and accounting systems for both the USDA and more than 60 other federal organizations. During fiscal year 1998, NFC processed more than $19 billion in payroll payments for more than 450,000 federal employees. NFC is also responsible for maintaining records for the world's largest 401(k)-type program, the federal Thrift Savings Program. This program, which is growing at about $1 billion per month, covers about 2.3 million employees and totaled more than $60 billion as of September 30, 1998.[6] The weaknesses we identified increased the risk that users could cause improper payments and that sensitive information could be misused, improperly disclosed, or destroyed.

- In October 1999, we reported that Department of Veterans Affairs (VA) systems continued to be vulnerable to unauthorized access.[7] VA operates the largest healthcare delivery system in the United States and reported spending more than $17 billion on medical care in fiscal year 1998. The department also processed more than 42 million benefit payments totaling about $22 billion in fiscal year 1998 and provided life insurance protection through more than 2.4 million policies that represented about $23 billion in

[5] DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk (GAO/AIMD-99-107, August 26, 1999).

[6] USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-99-227, July 30, 1999).

[7] Information Systems: The Status of Computer Security at the Department of Veterans Affairs (GAO/AIMD-00-05, October 4, 1999.)

coverage. In providing these benefits and services, VA collects and maintains sensitive medical record and benefit payment information for veterans and their family members. GAO, as well as the VA IG, continued to find serious problems that placed sensitive information at increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possible occurring without detection. For example, at one VA insurance center, 265 users who had not been authorized access had the ability to read, write, and delete information related to insurance awards. Such unauthorized access could lead to improper insurance payments.

POOR SECURITY PROGRAM MANAGEMENT IS THE FUNDAMENTAL CAUSE OF POOR COMPUTER SECURITY

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. We reported on this problem in 1996 and, again, in 1998,[8] noting that agency managers are not ensuring, on an ongoing basis, that risks are identified and addressed and that controls are operating as intended. In many cases, senior agency officials have not recognized that computer-supported operations are integral to carrying out their missions and that they can no longer relegate the security of these operations solely to lower-level technical specialists. For these reasons, it is essential that this fundamental problem be addressed as part of an effective information technology management strategy, which will also serve to strengthen critical infrastructure protection.

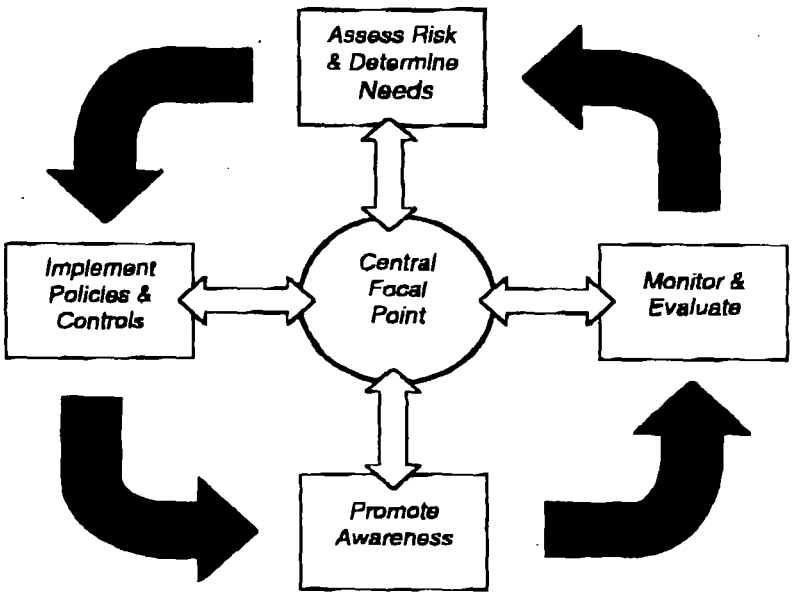
Agencies have responded to scores of recommendations for improvement made by us and by agency inspectors general. However, similar weaknesses continue to surface because agencies have not implemented a management framework for overseeing information security on an agencywide and ongoing basis. Instead, there is a tendency to react to individual audit findings as they are reported, with little ongoing attention to the systemic causes of control weaknesses.

[8]GAO/AIMD-96-110, September 24, 1996, and GAO/AIMD-98-92, September 23, 1998.

To identify potential solutions to this problem, we studied the security management practices of eight nonfederal organizations known for their superior security programs. We found that these organizations managed their information security risks through a cycle of risk management activities.[9] The basic framework—built on 16 specific practices—allows risk management through an ongoing cycle of activities coordinated by a central focal point. The management process involves

- assessing risk to determine information security needs;
- developing and implementing policies and controls that meet these needs;
- promoting awareness to ensure that risks, roles, and responsibilities are understood; and
- instituting an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective.

The Risk Management Cycle



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

The guide is generally consistent with OMB and NIST guidance on information security program management, and it has been endorsed by the CIO Council as a useful resource for agency managers.

One agency that has illustrated the value of these management practices in strengthening computer security is the Internal Revenue Service (IRS). The IRS has made significant progress by acknowledging the seriousness of its computer security weaknesses, consolidating overall responsibility for computer security management, reevaluating its approach to computer security management, and developing a high-level plan for mitigating the identified weaknesses.[10]

A COMPREHENSIVE STRATEGY FOR IMPROVEMENT IS NEEDED

While adopting the practices recommended by the guide can better prepare agencies to protect their systems, detect attacks, and react to security breaches, other actions are also needed to improve oversight and otherwise address the problem from a governmentwide perspective.

Presidential Decision Directive (PDD) 63, issued in May 1998, recognized that addressing computer-based risks to our nation's critical infrastructures requires an approach that involves coordination and cooperation across federal agencies and among public and private-sector entities and other nations. In this regard, PDD 63 established several entities to coordinate infrastructure protection efforts.[11] However, the details of the PDD's approach have not been finalized. As a result, a major objective of PDD 63 to make the federal government "a model to the private sector on how best to protect critical infrastructure," has not been realized nor is it clear how this objective will be met.

---

[10] IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk (GAO/AIMD-99-38, December 14, 1998).

[11] In May 1998, PDD 63 created several new entities in the National Security Council, the Department of Commerce, and the Federal Bureau of Investigation which also have responsibility for guiding and overseeing and coordinating agency security with a focus on critical infrastructure protection.

To provide greater assurance that critical infrastructure objectives can be met, we believe that actions are needed in seven key areas. I will briefly discuss each of these.

Clearly Defined Roles and Responsibilities

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating federal agency security, and the National Institute of Standards and Technology (NIST) with assistance from the National Security Agency (NSA) is responsible for establishing related standards.[12] In addition, interagency bodies such as the CIO Council and the entities created under PDD 63 are attempting to coordinate agency initiatives.

While these organizations have developed fundamentally sound policies and guidance and have undertaken potentially useful initiatives, effective improvements are not taking place. This is due, in part, to the relative immaturity of the recently established processes. It is also unclear 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.

Constraints on resources and the urgency of the problem require that government activities are designed and coordinated to achieve clearly understood goals. There must also be clear linkage between policy guidance, technical standards, and agency practices to ensure responsibility/accountability for actual improvements.

Specific Risk-Based Standards

Second, agencies need more specific guidance on the controls that they need to implement. Currently agencies have wide discretion in deciding (1) what computer security controls to

[12] The Computer Security Act and the Paperwork Reduction Act.

implement and (2) the level of rigor with which they enforce these controls. In theory, this is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data.

However, our studies of best practices at leading organizations have shown that more specific guidance is important. In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; and help ensure that shared data are appropriately protected. Implementing such standards for federal agencies would require developing (1) a single set of information classification categories for use by all agencies to define the criticality and sensitivity of the various types of information they maintain and (2) minimum mandatory requirements for protecting information in each classification category.

Routine Evaluations of Agency Performance

Third, routine periodic audits must be implemented to allow for meaningful performance measurement. A requirement for periodic examinations of controls in operation would significantly strengthen oversight requirements in the Computer Security Act, which focus on evaluating agency security plans, rather than practices.

Ensuring effective implementation of agency information security and critical infrastructure protection plans will require monitoring to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Evaluations at several levels can be beneficial. Tests initiated by agency officials are essential because they provide information needed to fulfill their ongoing responsibility for managing security programs. Evaluations initiated by independent auditors, such as agency inspectors general, can serve as an independent check on management evaluations and provide useful information for congressional and executive branch oversight. Summary evaluations performed by entities such as OMB, GAO, or the CIO Council can provide a governmentwide view of progress and help identify crosscutting problems.

At present, there is no requirement for periodic independently initiated tests and evaluations of agency computer security programs. As a result, information for measuring the effectiveness of agency security programs, and thus, holding agency managers accountable is limited. While some control testing is done in support of annual independent financial statement audits, ensuring routine periodic testing of all critical agency systems--both financial and nonfinancial—may require new legislation.

Executive Branch and Congressional Oversight

Fourth, the executive branch and the Congress must effectively use audit results and performance measures to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential to hold agencies accountable for their performance and was demonstrated by the recent OMB and congressional efforts to oversee the Year 2000 challenge.

Adequate Technical Expertise

Fifth, it is important for agencies to have the technical expertise they need to select, implement, and maintain controls that protect their computer systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. The Computer Security Act authorized NIST to provide assistance to agencies and included provisions for periodic training in computer security awareness and practice. However, as the Year 2000 challenge showed, the availability of adequate technical expertise has been a continuing concern to agencies.

A number of programs and recommendations have been proposed that merit congressional study. For example, prompted in part by concerns over technical staff shortages affecting Year 2000 efforts, the CIO Council's Education and Training committee studied ways to help agencies recruit and retain information technology personnel. The resulting report provides

an extensive description of the current status of federal information technology employment, improvement efforts currently underway, and detailed proposals for action.

Adequate Funding

Sixth, agencies must have resources sufficient to support their computer security and infrastructure protection activities. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks. Also, addressing the Year 2000 challenge has resulted in postponement of many program and information technology initiatives—including system enhancements and computer security.[13] OMB and congressional oversight of future spending on computer security will be important to ensure that agencies are not using the funds they receive to continue ad hoc, piece-meal security fixes not supported by a strong agency risk management framework.

Incident Response and Coordination

Seventh, there is a need to more comprehensively monitor and develop responses to intrusions, viruses, and other incidents that threaten federal systems. Several entities are already providing some central coordination in this area--including the FBI, NIST, and the FedCIRC.[14] However, the specific roles and responsibilities of these organizations, as well as the balance between governmentwide and individual agency responsibilities, should be clarified and expanded to provide a more comprehensive picture of the security events that are occurring and assistance in dealing with them.

Such efforts can take several forms that provide differing benefits. For example, a governmentwide response center could provide immediate emergency assistance to agencies

[13] Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999).

experiencing intrusions or other potential problems. It could also provide assistance on a non-emergency basis, especially by alerting agencies to new threats and vulnerabilities and helping them identify actions to prevent or mitigate incidents. By calling on a center for such assistance, agencies could tap into a source of specialized expertise that may be difficult and expensive to maintain at the individual agency level. A governmentwide center could also serve as clearinghouse of information on incidents that would be available to federal agencies and the public. Such information can be valuable in estimating the significance of different types of information security risks. For example, when the Melissa virus surfaced earlier this year, we found that there was no single place to obtain complete data on what agencies were hit and how they were affected. Moreover, there were no data available that quantified the impact of the virus in terms of productivity lost or the value of data lost.

Finally, it is important to recognize that, by itself, a central clearinghouse is not complete solution for the information security problems across the federal government. Agencies themselves must still use this information effectively to assess risks to their own computer-supported operations and to develop and implement sound management controls.

In conclusion, Mr. Chairman, I want to stress that there are no simple solutions to improving computer security throughout the government. What is clear is that a bottom up approach will not work. To begin to meet the lofty goal of PDD 63—making the government a model—will require sustained top management support, consistent oversight, and additional levels of technical and funding support. Taking steps to address the issues outlined in my statement could help the government put its own house in order and more effectively work with the private sector to protect critical infrastructures. This concludes my testimony. I will be happy to answer any questions you or Members of the Subcommittee may have.

(511065)

[14]FedCIRC—the Federal Computer Incident Response Capability—is a reporting center at the General Services Administration.

6 October 1999
Senate Judiciary Committee
Subcommittee on Technology, Terrorism and Government Information

Opening Remarks- Sen. Kyl
- see handout-

Opening Remarks- Sen. Feinstein
This is a critical and crucial area
New technology has lead to prosperity but with this power is a lot of danger
Have to balance global interconnectivity with security
Information warfare developed in about a dozen countries (ie. Lybia)
PDD63 CIP National Plan
- Time line already slipping. A report due last Dec has still not made it to Congress

Opening Remarks- Sen. Bennett (not part of subcom)
- see handout-

Testimony of John Tritak
*He started out going along with written testimony, but then appeared to run out of time around the education section
*No mention of R&D per se in his oral testimony
Key programs
$5 million for 15 member review team
$8.4 million for FIDNET
$17 million for education/ training
$7 million for government to government communication (public is the key)
$2 million for programs that foster information sharing

Testimony of Michael Vatis
- see handout –
Big problem is not knowing who you are dealing with

Questions
Kyl: Asked about the draft statement for the plan. Mentioned that one estimate of the damage of the 80-100 events daily in the first and second quarters of 1999 was $7 billion. Asked if anything could be said about this, people identified. (Mentioned the "Moonlight Maze" article from *Newsweek*)

Vatis: Moonlight Maze is the name of an investigation into intrusions in DoD and other government networks. Attacks appear to originate in Russia. Resulted in the theft of unclassified defense research matters.

Kyl: PDD63 issued in May 1998- now about a year over due. Are the plans completed? If not when? If so, when can Congress expect them?

Tritak: Plan in final stage of interagency review. Hope to issue at the end of October, beginning of November. 24 agencies involved. Do not think of plan as final, rather an invitation

to dialog. Need to engage private sector. Hopefully private sector and Congressional dialogue to follow.

Kyl: Have had to prod administration. *Read statement from Tritak testimony about (*A) FIDNET operating with in legal rules and then asked "Right???"

Tritak: Right.

Fein: DoD report 80-100 hackers attempt/ day. How many succeed?

Vatis: Don't know. Are many different types, including just pings.

Fein: What type of damage, if any, occurs?

Vatis: Generally just look around and taking unclassified information. Problem is access to information. Not much significant damage. Some has been done, but not sure.

Fein: Moonlight Maze, penetration of classified information?

Vatis: Can't discuss in this environment.

Kyl: Was supposed to be meeting with D. Clarke, will reschedule.

Benn: Really can't discuss this information because it is classified, but do need a follow-up.

Fein: Free software on the net that will help people leave invisible trap doors w/o detection.

Vatis: Several instances of this. One example is Back Orafice 2000, which permits external user to gain access. They have issued advisories. These things pop up daily.

Fein: Are there commercially available systems that can pierce classified information.

Vatis: Security for classified information is mostly done thru lack of access.

Fein: Would like to discuss in a classified meeting too. What is appropriate regulation (if any) of systems that can pierce privacy...? Any suggestions?

Vatis: Are many security measures that are basic- just need resource and attention. Examples: personnel security, smart cards, up date virus detection, implement patches.

Fein: Are protection measures in place in key government systems now?

Vatis: Basically, yes. Breakdowns occur at implementation.

Fein: What about private sector?

Vatis: Government has very little authority to mandate. They have begun to spend the money to do this, but is still a problem.

Fein: Of these, what's the level of vulnerability?

Vatis: High

Fein: *Mentioned the SF example again. In private sector there is high vulnerability and private sector hasn't responded significantly?

Vatis: Mixed bag, but generally no. Is reason trying to promote information sharing. Don't want to make it seem like private is bad and government is good. Government has problems too.

Benn: *Mentioned July committee hearing on cyber reconstitution and how to facilitate.

Vatis: Reconstitution of private is responsibility of private sector with public assistance.

Benn: Maybe have something in place to help them. Concern is people who go undetected. Have people gotten in and out without our knowledge and left trap doors. Private things, hey not a problem. Progress has been made when gotten the attention of CEO. How effective are private firewalls compared with government?

Vatis: Varies.

Benn: Hypothetical situation. Suppose there was a government red team set up to offer to attempt to break into private industry. How would private sector react?

Vatis: Some welcome, some against.

Benn: What about government agencies?

Vatis: Red team is important to security. Should be done.

Fein: At least 22 agencies have significant weaknesses according to GAO. Have these been remedied?

Vatis: Don't know.

Tritak: Don't know.

Kyl: Please submit additional questions for the record. Want plan timing completion report, etc. Would be beneficial to have possible cases that show examples of different types of break-ins- walk them through the cases.

Testimony of Jack Brock

- see handout-

Questions

Kyl: Through GAO audits have found "government is not adequately protecting..." that there are persistent weaknesses over the past 5 years. Just this year DoD weapons research etc. has already been impacted. This needs to be conveyed to public. In the attacks done by GAO has classified information been accessed?

Brock: Only go after unclassified.

Kyl: Why has PDD63 taken so long?

Brock: Starting from environment without consensus. Each agency had to develop plan from ground zero. Logistics problems- inability of agencies to provide information required.

Kyl: Give us suggestions. Recommend to the Chair of the Government Op. Committee to review GAO audits and begin to bring in agencies who don't get things fixed. What else can we do?

Brock: Constant spotlight.

Fein: Money just isn't available from government. Do we have expertise to do what is necessary? How do we get cutting edge knowledge that we lack? We can't get a new roof unless people understand.

Brock: National plan contemplating sponsoring R&D, education, look at ways of attracting more people. Possible contract out with proper controls. A lot at can be done at no cost- control discussions on Internet. Many people get access through password guessing because people use short ones and are lax in changing them. Fed Reserve is VERY good. Management attention is most critical.

Fein: Want full list of things found in audits. Want them to go back in one month and see if remedied. Bet not.

Brock: Can give overview and details.

Kyl: Consider letter to president as he considers his budget. Need to look at recommendation of agencies regarding this issue.

Fein: Should be required to report incidents.

Brock: Many do not report.

Botz: There is no common definition of what an incident is.

Kyl: Agree with Fein. We need to try and put this in the plan, if not then through legislation. All need to be reported so can help stop.

Fein: Draft letter to Tritak to have this put in plan.