Case Number: 2008-0702-F

FOIA MARKER

This is not a textual record. This is used as an administrative marker by the Clinton Presidential Library Staff.

Folder Title: Cybersecurity Remarks [3]				
Staff Office-Individual: Speechwriting-Orzulak, Paul				
Original OA/ID Number: 4022				
Row: 48	Section: 6	Shelf: 9	Position: 2	Stack: V

```
****------------------------------------------------------------------------****

*      19 PAGES                618 LINES              JOB  90867   105D6C      *
*  12:31 P.M. STARTED    12:32 P.M. ENDED                 01/06/00              *
****------------------------------------------------------------------------****
****------------------------------------------------------------------------****
*                          EEEEE      N   N      DDDD                          *
*                          E          N   N      D   D                         *
*                          E          NN  N      D   D                         *
*                          EEE        N N N      D   D                         *
*                          E          N  NN      D   D                         *
*                          E          N   N      D   D                         *
*                          EEEEE      N   N      DDDD                          *

****------------------------------------------------------------------------****

****------------------------------------------------------------------------****
```

SEND TO: ORZULAK, PAUL
DEPT. OF HOUSING & URBAN DEVELOPMENT
OFFICE OF POLICY SUPPORT
451 7TH ST. SW - ROOM 10132
WASHINGTON, DISTRICT OF COLUMBIA 20410

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release September 16, 1999

PRESERVING AMERICA'S PRIVACY AND SECURITY IN THE NEXT CENTURY: A STRATEGY FOR AMERICA IN CYBERSPACE

A REPORT TO
THE PRESIDENT OF THE UNITED STATES

September 16, 1999

William Cohen
Secretary of Defense

Janet Reno
Attorney General

Jacob J. Lew
Director of the Office
of Management and Budget

William Daley
Secretary of Commerce

PRESERVING AMERICA'S PRIVACY AND SECURITY IN THE NEXT CENTURY: A STRATEGY FOR AMERICA IN CYBERSPACE

1. A TIME OF PIVOTAL CHANGE

American history has been punctuated by periods in which the Nation had to respond to sweeping social, economic and technological developments. In the best of times, people working together in government and industry became the engine of progress that shaped the character of the time and facilitated new prosperity and opportunity for Americans. Three examples illustrate this point.

Opening the Heartland and expanding the frontier. Beginning with the Louisiana Purchase in 1803, the government initiated a remarkably successful policy to open up a vast new area. Over the next five decades, the United States doubled the size of its territory. Under the government's plan, land grants were given to railroads to open the

Midwest and in turn to create a future market for rail services. Land was awarded to homesteaders, and yet other parcels were reserved as income sources for institutions of higher education.

The technological advance of the railroad was the engine pulling this growth. From the 1820s to 1900, American railroads added an average of more than 2,000 miles of track each year. By the close of the 19th century, the combination of these factors had served to triple the size of our nation. The Administration and the Congress, working together and in concert with technology advances, created an infrastructure for a new society.

Industrialization and the Great Depression Produce a New Society. Around the turn of the century, the country was firmly in the Industrial Age. Technical innovations in automation and machinery spurred the growth of factories, assembly lines and mass-production in our nation's cities. The Ford assembly line for the Model T and the Wright brother's flight catapulted us into a mobile society and drove further technological innovations. Telephones became more commonplace and the nation began to shrink as news and information traveled faster. As a nation, we created new opportunities in industries never heard of, and created a new class of wealth, based on opportunity and innovation, not birthright. The economy moved from an agrarian society to an industrial society.

But the growth and prosperity experienced by many halted when the Great Depression gripped the country. In response, the government developed a series of creative policies and programs that brought government and business to the common task of restoring productivity to America. While there were a number of social programs, government support for technology was key to driving development. For example, the government took a pivotal role in expanding the electrical grids that would become the backbone of our national infrastructure, first with the creation of the Tennessee Valley Authority in 1933 and two years later with the creation of the Rural Electrification Administration. Electrical technology, in the ensuing years, radically altered the capabilities of America's rural farms and industry. Just as important, it created a transmission belt that further disseminated the ideas and technology being generated in the nation's cities.

A World War Produces a Global Community and the American Century. In a third case, World War II shattered the international political system at the same time that it brought an end to 19th century colonialism. The creation of the World Bank, the International Monetary Fund, and the rules for a global trading system became the cornerstones of the emerging global economy.

The urgent need for increased production and the burst of scientific funding associated with the war effort -- sustained by a continuing Federal commitment to new science and technology in the following years -- vaulted the United States into the age of electronics and computers - the beginning of the Information Age.

Advances in telecommunications, such as broad-band carrier systems and switching devices, combined with innovations in the computer industry to give individuals more power than ever to process large amounts of information and transmit that information at ever-greater speeds. Further, this country's goal to reach the moon by the end of the 1960s fueled development of advanced electronics, increased computing power and communications capabilities. At the same time, technological leaps in computer memory and data storage enabled the centralized use (and, unfortunately, misuse) of information to examine or profile individuals, consumers, and groups. As these issues emerged, our legal system responded. Looking back, the "Information Economy"

that Americans recognize today could be seen emerging as early as the late 1940s.

Each of these examples was a pivotal episode in American history in which complex social, economic, and technological forces came together. Facing the challenges of the day, America's governmental, societal and technical leaders crafted a new vision of the future, and in the process became pioneers on a new frontier of opportunity and promise.

America now faces a new time of pivotal change, enormous opportunity, and promise. This time, technology itself presents both an opportunity and a threat to global society increasingly dependent on, and connected by, advanced computing and communications. Continuing a balanced strategy that advances our national interests is the challenge of our day.

2. Cyber America: Great Promise and Serious Risks

America now stands on the brink of revolution fueled by machines - computers - and networks of computers that facilitate the instant exchange of and access to ideas and information. The computer has and will continue to revolutionize virtually all aspects of American society, just as electricity, the power grid and the railroad changed our forefathers' society.

The Computer as an Economic Engine. It is well known that the computer, and its application in business, commerce, education and recreation has transformed the American economy. America is becoming a country of "knowledge workers," with the ubiquitous application of computer technology at its core. America's productivity today is grounded in computer applications and networks. Barcodes speed us through shopping lines and simultaneously facilitate store manager recordkeeping and reordering. Airline reservations can be booked from home computers. Everything from clothes to books to software can be purchased over the Internet. American companies are discarding their proprietary computer systems and using the Internet and the Web to increase productivity, network their entire chain of suppliers, and deliver "just-in-time" training to their employees. American students can conduct original research with colleagues on machines around the world with but a few keystrokes. Travelers can monitor current weather conditions in another country. Scientists can "conference" electronically and transmit astounding volumes of information in seconds to colleagues on other continents.

As remarkable as today's innovations are, the years ahead hold even greater promise. Computers will become virtual partners in all aspects of our lives. Homes will be centrally wired to allow integrated alarms, electronics, appliances, telephones, and computers to simplify our lives. Education will become more adaptive to the routines of individual students, and banking, finance, and shopping will increasingly migrate to the home and portable computing devices.

And in this process and through networking, computers have created the well-known "cyberspace" that eliminates the traditional boundaries of time and place and links governments, businesses, and individuals in the same electronic environment.

The Dangers of Cyberspace. Like any new tool in previous eras, computers can be used by those who prey on the innocent. International narcotics traffickers now routinely communicate with each other via computer messages. Hostile governments and even some transnational organizations are establishing cyber-warfare efforts, assigned the mission of crippling America's domestic infrastructure through computer attacks. Hackers destroy cyber-property by defacing homepages and

maliciously manipulating private information. Pedophiles stalk unsuspecting children in computer chat rooms. Individuals post homepages with instructions to manufacture pipebombs, chemical weapons, and even biological agents. Crooks break into business computers, either stealing funds directly or extorting payments from companies anxious to avoid more expensive disruption. Disgruntled employees, with valid access to their companies' system, can take steps to disrupt the business operations or steal proprietary, sensitive, and financial information. And our personal data is at risk of being unlawfully accessed and read by malicious individuals, without our knowledge, as it resides on or traverses communications and computer networks.

These concerns are not hypothetical. We have seen these types of activities, and other equally dangerous activity, in past and on-going cases. The danger posed by evil individuals using these powerful new tools grows by the day. Just as other technologies have the risk of being abused, it is necessary for us to evaluate how to respond. Without protective action, we will not be safe. America must take responsible steps to ensure that this promising electronic environment is safe for law abiding citizens and businesses.

3. Balancing America's Bedrock Values

While these problems seem unprecedented, in fact they represent a return to the bedrock problems faced by America's constitutional founders. American democracy became and remains a new experiment in government--balancing the rights of individuals against the imperatives of society and limiting the reach of government into personal, private lives, while mandating a government responsibility for public safety and security for all citizens.

Computers are now at the center of competing American values. In honest, law abiding citizens' hands, the computer becomes an indispensable tool for education, personal and commercial business, research and development, and communications. In criminal hands, the same computer becomes a tool of destruction and criminality.

Enter encryption. Over the past decade, another information technology has emerged that amplifies this tension - encryption. Encryption includes special instructions that scramble a clear readable message in complex ways that make it unreadable. For the strongest forms of encryption, only the intended recipient can unscramble the message and read the original plain text, unless someone else has gained access to the corresponding decoding software and decryption key.

Originally only available and used by military agencies, strong encryption is now available to many and has become a building block for the new digital economy. It is essential to provide security and privacy for electronic commerce and e-business. Encryption is critical because it allows individuals, businesses, and other organizations to share information privately without it being unlawfully intercepted or accessed by a third party, to establish their identities, and to maintain the integrity of information. Without the use of encryption, it is difficult to establish the trust that people and firms need to do business with each other, or to have confidence to run their business electronically. With the use of encryption:

- Individuals and consumers can securely conduct their finances and communicate with each other over the Web.

- Firms can transmit their software, music, movies, reports and other forms of intellectual property over the Internet while minimizing the risks of widespread piracy.

- Businesses can protect their company proprietary information over the Internet, with confidence that the information is secure from prying eyes.

- Firms can develop products more rapidly, as teams of engineers around the world can collaborate on their designs in real-time over secure high-speed networks.

However, while the majority of users will use encryption for legitimate, lawful purposes, we must recognize that terrorists, pedophiles and drug gangs are increasingly using encryption to conceal their activities. Hence, encryption has posed a serious public policy challenge over the past decade.

The Federal Government has sought to maintain a balance between privacy and commercial interests on one hand and public safety and national security concerns on the other by limiting the export of strong encryption software. Preserving this balance has become increasingly difficult with the clear need for strong encryption for electronic commerce, growing sophistication of foreign encryption products and the proliferation of software vendors, and expanded distribution mechanisms. In the process, all parties have become less satisfied with the inevitable compromises that have had to be struck. U.S. companies believe their markets are increasingly threatened by foreign manufacturers in a global economy where businesses, consumers, and individuals demand that strong encryption be integrated into computer systems, networks, and applications. National security organizations worry that the uncontrolled export of encryption will result in diversion of powerful tools to end users of concern. Law enforcement organizations see criminals increasingly adopting tools that put them beyond the reach of lawful surveillance.

At the end of the century, these are the important national interests that must be reconciled. Determining a policy direction for encryption has become more complex, and more urgent, for all those affected. A strategic paradigm that better achieves balance is needed.

4. A New Paradigm to Protect Prosperity, Privacy and Security

To support America's prosperity and protect her security and safety, we propose a new paradigm to advance our national interests. The new paradigm should be comprised of three pillars - information security and privacy, a new framework for export controls, and updated tools for law enforcement. We discuss each in turn.

I. Information Security and Privacy. As a nation, we have become increasingly dependent on computers and telecommunications. These new technologies create vast opportunities for personal expression and electronic commerce, while also creating new risks to public safety and national security. Computers and telecommunications rely on open protocols and ultra-accessibility, thus making individuals' and organizations' words and actions vulnerable to outsiders in new and potentially frightening ways. A first pillar of our new paradigm must be to promote information security and privacy - to assure the security and privacy of stored and transmitted data from unauthorized and unlawful access.

The President has recognized the challenge of updating privacy for new technologies: "We've been at this experiment in Government for 223 years now. We started with a Constitution that was rooted in certain basic values and written by some incredibly brilliant people who understood that times would change, and that definitions of fundamental things like liberty and privacy would change, and that circumstances

would require people to rise to the challenges of each new era by applying old values in practical ways."

In updating enduring constitutional values for the computer age, we need to assure that our citizens' personal data and communications are appropriately protected. Businesses need to privately communicate with their employees and manufacturing partners without risk that their proprietary information will be compromised through unauthorized access. Encryption is one of the necessary tools that can be used in this technological environment to secure information. Therefore, we encourage the use of strong encryption by American citizens and businesses to protect their personal and commercial information from unauthorized and unlawful access.

We must also recognize the inherent security risks posed by the spread of and dependence on "open systems" and ready accessibility. The Defense Department's situation is typical. Twenty years ago the Defense Department operated largely proprietary communications systems over government owned switches and circuits. DOD technology was homebuilt and tightly controlled. Today, the U.S. DOD has more computer users than any other organization in the world - 2.1 million computers access over 10,000 networks on an average work day. Even so, 95% of DOD's communications occur over public circuits or with commercial software and hardware. The Defense Department's reliance on commercial products and services is repeated throughout the country by government agencies and the private sector.

If the Department of Defense is to function safely in cyberspace, it must use strong tools for encryption and identity authentication. It is not just military operations and data that must be protected. All government agencies and all business activities will increasingly need a full set of security tools to ensure access, privacy and absolute confidence in business operations that utilize computer technology.

We recognize that information technology is changing rapidly and constantly providing both new security capabilities and challenges and, hence, we will never reach a "perfect solution." Nevertheless, there are many efforts underway throughout the government to address the need for more secure systems. By adopting commercial approaches, where appropriate, and sponsoring R&D to fill needed capabilities, we believe the Federal government should, by example, lead the way for America to develop and use the tools and procedures for information security and privacy in the next century.

The Department of Defense, for example, has allocated over $500 million to develop a comprehensive security management infrastructure. This infrastructure will utilize a range of encryption products (with stronger products for more sensitive applications involving higher levels of classification), and a public key infrastructure (PKI) to identify and authenticate those who use our information networks. The Department is also adopting stronger standards for network configuration and operator qualification and certification, and is taking steps to better detect unauthorized intrusions into DOD networks.

The Federal government must continue to promote the development of stronger encryption technologies for federal use. The advanced encryption standard (AES) is in the final stages of a public selection process. Once promulgated, AES could become as ubiquitous as today's digital encryption standard (DES) which has contributed greatly to the growth of electronic commerce.

In the Federal government, the Department of Defense is a leading proponent of information security through its information assurance initiative, and other agencies are recognizing the need for increased

diligence in maintaining adequate security of Federal information and systems. We encourage each agency to vigilantly build security enhancements into their business operations in risk-based and cost-effective ways that enable, not impede, the agency's ability to perform its mission.

Further, we believe that the Congress and Executive Branch should work together to promote both the awareness of information privacy and security and the development of appropriate tools and resources by the private sector, and to consider whether tangible incentives are appropriate. Given the rapid changes in technology, we advocate a technology neutral approach. This approach would have the public and private sectors working together to encourage development of a broad range of privacy and security products and processes and share promising practices with one another. We believe equally strongly that security infrastructures and the deployment of security products -- should neither be mandated nor prohibited. Public and private organizations must determine their risks and be free to choose their own solutions.

The government's requirement to protect its own sensitive and privacy information is matched by individual's and the private sector's own interests in proper handling of sensitive information. Many in industry and elsewhere are already developing and using sophisticated security and privacy products and processes. Government should act as a facilitator and catalyst and help stimulate the development of commercial products that will help all Americans protect their sensitive information.

In sum, the first pillar of the new paradigm calls on the Federal government, the Congress and all others to partner in promoting ways to bring information security and privacy to the Information age. Working together, we can develop tools and procedures for safe operation in cyberspace, applying enduring constitutional values to our new circumstances.

II. Encryption Export Controls for the New Millennium. At the dawn of the new millennium, technology is advancing at such a rapid pace that attempts to control its global spread under the existing export control regime need to be regularly reevaluated. Encryption will continue to enable new economic realities that must be considered in a balanced approach to export controls.

Encryption products and services are needed around the world to provide confidence and security for electronic commerce and business. With the growing demand for security, encryption products are increasingly sold on the commodity market, and encryption features are being embedded into everyday operating systems, spreadsheets, word processors, and cell phones. Encryption has become a vital component of the emerging global information infrastructure and digital economy. In this new economy, innovation and imagination are the engines, and it is economic achievement that underpins America's status in the world and provides the foundation of our national security. We recognize that U.S. information technology companies lead the world in product quality and innovation, and it is an integral part of the Administration's policy of balance to see that they retain their competitive edge in the international market place.

We as a nation must balance our desire and the need to assist industry with a prudent, objective and steady judgment about how to protect national security; a judgment that acknowledges that technological advantages may add new dimensions to an already complicated problem set. We must ensure that the advantages this technology affords us are not extended to those who wish us ill or who harbor criminal intent. This judgment must be informed by both foreign

and domestic realities.

While the U.S. is a huge market for telecommunications goods and services, the other nations of the globe present markets much larger than our domestic demand. Our networks are inextricably bound to those of our allies and adversaries alike. Likewise, America's interests do not end at our borders. American diplomats, service men and women, as well as countless business people work and live around the globe. America's interests are served by the ability to send and receive proprietary, personal and classified information to exactly where it is needed around the world. Likewise, America's interests are served daily by shared actions with our allies, which require accurate and authentic information be exchanged. Our policy must acknowledge these vital interests.

But even as we do, it is imperative that we uphold international understandings, and strive with other nations to prevent the acquisition of encryption technology to sponsors of terrorism, international criminal syndicates or those attempting to increase the availability of weapons of mass destruction. We must also meet our responsibilities to support our national decision makers and our military war fighters with intelligence information in time to make a difference.

Accordingly, the Administration has revised its approach to encryption export controls by emphasizing three simple principles that protect important national security interests: a meaningful technical review of encryption products in advance of sale, a streamlined post-export reporting system that provides us an understanding of where encryption is being exported but is aligned with industry's business and distribution models, and a license process that preserves the right of government to review and, if necessary, deny the sale of strong encryption products to foreign government and military organizations and to nations of concern. With these three principles in place, the Federal Government would remove almost all export restrictions on encryption products. This approach will provide a stable framework that also will allow U.S. industry to participate in constructing and securing the global networked environment. This approach also maintains reasonable national security safeguards by monitoring the availability of encryption products and limiting their use in appropriate situations.

The Administration intends to codify this new policy in export regulations by December 15, 1999, following consultations on details with affected industries and other private sector organizations.

However, with this new framework for export controls, the national security organizations will need to develop new technical tools and capabilities to deal with the rapid expansion of encrypted communications in support of its mission responsibilities. The Congress will need to support such new tools and technical capabilities through necessary appropriations.

III. Updated tools for Law Enforcement. Because of the need for and use of strong encryption globally, governments need to develop new tools to deal with the rapid expansion of encrypted communications. Updated tools for law enforcement that specifically address the challenges of encryption constitute the third pillar of the new strategy. We cannot ignore the fact that encryption will be used in harmful ways - by child pornographers seeking to hide pictures of exploited children, or commercial spies stealing trade secrets from American corporations, or terrorists communicating plans to destroy property and kill innocent civilians. Even more significant, because cyberspace knows no boundaries and because it is not immediately clear if a cyberattack involves Americans or foreigners, America's national security will increasingly depend on strong and capable law enforcement

organizations. This is because the United States military and intelligence agencies have long been restricted by law from undertaking operations inside the United States against American citizens. Accordingly, America's national defense is now increasingly reliant on ensuring that our law enforcement community is capable of protecting America in cyber space.

Under existing law and judicial supervision, law enforcement agents are provided with a variety of legal tools to collect evidence of illegal activity. With appropriate court orders, law enforcement may conduct electronic surveillance or search for and seize evidence. In an encrypted world, law enforcement may obtain the legal authority to access a suspect's communications or data, but the communications or data are rendered worthless, because they cannot be understood and cannot be decoded by law enforcement in a timely manner. Stopping a terrorist attack or seeking to recover a kidnapped child may require timely access to plaintext, and such access may be defeated by encryption. Hence, law enforcement's legal tools should be updated, consistent with constitutional principles, so that when law enforcement obtains legal authority to access a suspect's data or communications, law enforcement will also be able to read it.

Quite simply, even in a world of ubiquitous encryption, law enforcement with court approval must be able to obtain plaintext so that it can protect public safety and national security. Therefore, we must undertake several important and balanced initiatives.

First, we need to ensure that law enforcement maintains its ability to access decryption information stored with third parties, but only pursuant to rules that ensure appropriate privacy protections are in place. To ensure this result, the Administration and the Congress must develop legislation to create a legal framework that enhances privacy over current law and permits decryption information to be safely stored with third parties (by prohibiting, for example, third party disclosure of decryption information), but allows for law enforcement access when permitted by court order or some other appropriate legal authority.

Second, since criminals will not always store keys with third party recovery agents, we must ensure that law enforcement has the personnel, equipment, and tools necessary to investigate crime in an encrypted world. This requires that the Congress fund the Technical Support Center as proposed by the Administration, and work with the Administration to ensure that the confidentiality of the sources and methods developed by the Technical Support Center can be maintained.

Third, it is well recognized that industry is designing, deploying and maintaining the information infrastructure, as well as providing encryption products for general use. Industry has always expressed support, both in word and in action, for law enforcement, and has itself worked hard to ensure the safety of the public. Clearly, industry must continue to do so, and firms must be in a position to share proprietary information with government without fear of that information's disclosure or that they will be subject to liability. Therefore, the law must provide protection for industry and its trade secrets as it works with law enforcement to support public safety and national security. The law must also assure that sensitive investigative techniques remain useful in current and future investigations by protecting them from unnecessary disclosure in litigation. These protections must be consistent with fully protecting defendants' rights to a fair trial under the Constitution's Due Process clause and the Sixth Amendment.

The Administration and the Congress need to work jointly to pass legislation that provides these updated authorities. The Administration

is in the final stages of drafting legislation and will shortly submit it to the Congress for consideration.

It is imperative to emphasize that the malicious use of encryption is not just a law enforcement issue - it is also a national security issue. The new framework for export controls must be complemented by providing updated, but limited authorities to law enforcement.

5. Conclusion

America stands on the pivot point of a crucial time in its ongoing development, and we face once again the on-going debate in this country between individuals' rights and the collective needs of society. The genius of our Constitution is in the balanced way it addressed that debate and in the procedures it created for continuing that discussion as the society and the economy evolved. For our own part, we enter that debate determined to preserve that same balance of the rights and responsibilities that has characterized our country through its history, but we are equally determined not to be thoughtlessly bound to old approaches and old technologies. Our challenge is to adapt our historical approach to the technological challenges we face. We believe the new paradigm described above achieves that objective.

We can now see a future with great promise and - and serious consequences - posed by the same technical developments. How well we handle these important challenges will shape the next century. It is far better that we approach these problems from a cooperative perspective. The past years of confrontation must be replaced by an era of collaboration. For only by working together, which is the rich history of this nation, can we ensure our economic viability and protect ourselves from those who would do us harm.

# # #

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release December 28, 1999

INTERVIEW OF THE PRESIDENT
BY CHARLIE ROSE OF 60 MINUTES II

The Oval Office
December 22, 1999

5:10 P.M. EST

Q Mr. President, because of the recent arrest and heightened security concerns at airports, do you expect, worry, that there will be an incident of terrorism before the first of the year?

THE PRESIDENT: Well, we are on a heightened state of alert and we're doing a lot of work on this. But l would say to the American people, they should go on about their business and celebrate the holidays as they would, but they should be aware. You know, this whole millennial idea draws out a lot of people who are maybe, by our standards, deranged, and other people maybe want to use if for their own political ends. So if people see anything suspicious, they should report it to the authorities as quickly as possible. But otherwise, I should say, they should go on about their business. We're working very, very hard on this.

Q It worries you?

THE PRESIDENT: No, I'm concerned, but I think we have, I think, t best law enforcement folks we could have and they are working very hard. And we're doing quite well so far. So I have every hope that we'll get through it. But I think that what I would ask the American people to do is not to stay at home and hide, but just to keep their eyes open. If they see something that looks fishy, tell the authorities and we'll get on it. But they should know that we're working this very hard.

Q All right, let me -- I look around this office and I see a desk over there that President Kennedy sat at. And I remember the story he said about the presidency, and one of the great things about the presidency was he could walk to work. As you think about leaving this building, what will you miss the most?

THE PRESIDENT: I think what I'll miss the most is the work, the job, the contact with all kinds of people and all kinds of issues, the ability to make a difference, to solve problems, to open up opportunities for other people. There's almost no -- not almost, I suppose there is no job like it in t world. It's been an unbelievable thrill and a profound honor, and I will miss it very much.

I'll miss a lot of the other things. I love living in the White House. Hillary I suppose has done more work on the White House than anybody since the Truman administration, redoing rooms and building a sculpture garden and doing things like that. And we love living here. I love going to Camp David; I love Air Force One; I love all of the perks of the job. But the thing I love most is being President, doing the job every day. It's just - to me, it's an almost indescribable

honor. I would never grow tired of it and I feel graced every day.

Q If you could change the 22nd Amendment, would you?

THE PRESIDENT: I don't know. It's probably not fair to ask. On balance, I think the two-term tradition has served us well. I'm glad President Roosevelt served the third term, because of the war. But on balance, I think it's served us well.

Now, you know, I'm young and I'm strong and I'm, as far as I know, in good health. I love the job. And so if I could serve again I probably would. But I think that's the reason we have this limit, so that people like me don't get to make that decision. (Laughter.)

Q Are you going to leave a note in that desk over there for your successor, and what will you say?

THE PRESIDENT: I will, and I don't know what I'll say. But -- probably most of what I'll say will be predictable. I'll be wishing my successor well and talking a little bit about the job, and offering to be available if I can ever be of any help.

Q Prosperity. Economic prosperity and growth has been a hallmark of this presidency. How long can it last, and will it be a part of our future, our near future?

THE PRESIDENT: Well, it certainly will be part of our future. Now, how long it will last -- the truth is no one knows. I believed when I got here that there was a chance that we could have a very long period of economic growth. Now, I couldn't have known when we started and we started slashing the deficit and investing more in technology that we would have the longest economic expansion in history that would even outstrip wartime when we had been fully mobilized. And in February we will. But I think that there are some fundamentally different things now.

If the government can follow good policies and the Federal Reserve will follow smart policies, there is this enormous power of productivity we're getting out of the revolution in technology and information technology. It's just now working its way into every sector of the economy, and it's also continually advancing itself. So I think if we can keep that going, and if we can keep our markets open -- that's very important; not just the exports we sell, but the imports we buy, the open market keeps the American economy highly competitive and tends to keep inflation down. And I think that's one of the things that's been under-appreciated about this.

I never will forget, back in '94 I got really alarmed when lumber prices went way up in a hurry, and I thought home-building prices were going to explode. And then all of a sudden, we had this big infusion of less costly imports. Now, we have to work on fair trade rules; we've got to have -- we can't be taken advantage of, as some tried to during the Asian financial crisis, but on balance, these open markets are very good for us. They give us growth and competition, keeps inflation down. And I think that's very good.

Q What we want to do here in this conversation is really focus on the future. You've done a number of conversations about this century and your term in office. Thinking about the future and the economic health of the country, there is also this process. In 10 years -- 10 years ago the wall came down; five years ago the web went up. Globalization is part of our life.

THE PRESIDENT: It is.

Q Some worry -- and Seattle might be an indication that we're looking at the possibility of a great gap between a two-tier system, between the haves and the have nots of the world, those who get it with technology and those that don't.

THE PRESIDENT: Well, first of all, the worry is well-founded, but it's a constant. That is, we have had a great gap in opportunity, even though it's sometimes closed and sometimes open, but there has been a huge gap between the haves and have nots since the dawn of the Industrial Revolution and the creation of middle class societies with mass wealth. Some have had it and others have not ever created it.

There is a chance that what will happen now is that it will become more pronounced across countries and within countries because of the advantages that technology-literate people and entrepreneurs with access to money will have in a rapidly changing world. That is, it's liable to accelerate.

But I would remind you that in the United States we had an increasing gap between the rich and the poor for about 20 years, as we moved into this new economic phase. The same thing happened when we changed from being an agricultural economy to an industrial economy. In the last two or three years, we started to see the gap close again. And the answer is not to run away from globalization; the answer is to make change our friend. The answer is to have broad access to information and information technology; to have broad-based systems of education and health care and family supports in every country; and to continue to try to shape the global economy.

You mentioned Seattle. I think that you had a lot of people out there protesting globalization, but they can't reverse it, and it's done a lot more good than bad. It's created, over the last 50 years, as the world had become more interconnected, we've moved away from the specter of war as holocaust, even though there have been a lot of smaller wars, and we've seen millions -- hundreds of millions of people lifted into the middle class. So the answer is how to make this globalization more human, more humane, and how to shape it so that everybody has a chance to be a part of it.

Q But you hear around the world now, as I'm sure you've heard from heads of state and others, this kind of unilateralism, America in the future is too strong, too dominant, and the fear of a backlash against us.

THE PRESIDENT: I agree with that. And I think -- I've tried to be very sensitive to that. I think we have -- and to make sure that we fulfill our responsibilities. I think that, on the one hand, people are glad that we won the Cold War, if you will; they're glad that the forces of freedom won. All over the world people are embracing democracy and market economics. But if you enjoy the level of military and economic strength we have, and the level of political influence, people are going to resent you.

And I must say -- and again, I don't mean to be partisan here, but I think t resentment is deeper when the Congress takes as long as they did to pay our U.N. dues and puts the conditions on it they did; when we don't ratify the Comprehensive Test Ban Treaty; when we basically preach to other people around the world, you ought to do this, that or the other thing, but instead of helping them, we continue to have a very large military budget, but we spend the smallest percentage of our income on assistance to other countries to help them succeed economically and politically of any advanced country in the world.

So we do some things that breed this resentment. Now, a lot of them resented me at Seattle because they think that when the United States says we ought to have core labor standards and we ought to have good environmental standards in a world trading system, that I'm trying to keep poor countries down, that I just want them to open their markets to us, but they won't get rich because I'm going to try to force them to give up their comparative wage advantage or their ability to grow. That's not true. So some of the resentments against America are not fair. But it's all perfectly understandable. I mean, look how fortunate we are compared to most other countries. And when people get in a tight they want us to come help -- Bosnia, Kosovo, the Middle East, you name it.

Q Do you think this century coming up will be America's century, as the 20th century has been described?

THE PRESIDENT: Well, I think it can be. But I think we have to think very carefully about how we want to define that. I mean, look what we know will happen. We know that, barring some completely unforeseen event, China, and sometime thereafter, India, will have economies that look bigger than ours, because they've got so many more people than we do -- four times as many people -- in the case of China, even more. We know that Europe will grow more integrated, I think, in the 21st century. And the European Union will be more and more a union. And they have 50 percent more people than we do -- and they could have a lot more than that if they continue to bring in other countries.

So I do not believe that we will have the relative economic dominance we have today. We've got about 4 percent of the world's people and almost 22 percent of the world's income. But I think we can be still very prosperous. I think we can still be the strongest individual country in the world in many ways. But I think we will have to build partnerships with some of those who resent us now. We will have to have an increasingly interdependent world. Because, whether we like it or not -- it's like globalization, interdependence is another word for globalization -- we will become more interdependent and we'll have to learn to be adroit at that. We won't be able to just say, well, if we like it, we're here and if we don't we'll walk away. We'll have to really work on our partnership skills.

Q You touched on something that I've thought about. This century was marked by our friends becoming our enemies -- France and Germany; our enemies becoming our friends. Is that going to be part of the 21st century, people we now look on as rivals become friends, friends become --

THE PRESIDENT: I think it is highly likely that some of the people that have been our most recent rivals will be our friends.

Q Like?

THE PRESIDENT: Well, I know a lot of people are very skeptical about Russia now, because of the problems they've had. But they just had a genuinely democratic election with a lot of debate, vigorous opposition, brutal campaign ads, you know, the whole nine yards.

Q Did the results surprise you?

THE PRESIDENT: No. It's about what I thought they'd be. You know, still only 25 percent of them are voting for the old Communist Party -- the rest of them are for something else, in spite of the economic hardship that they have faced in the last few years.

So I still think there's a chance that if the leaders of Russia

define their national greatness in 21st century terms -- that is, in terms of their ability to unleash the creative capacity of their people, rather than their ability to dominate their neighbors, which was their 19th and 20th century definition of greatness -- that they well be -- we'll have a real partnership there. It's also possible that we'll have one with China.

Q A partnership?

THE PRESIDENT: Absolutely. It just depends on how they view us and their own self-interest.

Q Do you see, on the other hand, people who we might consider friends, like Western Europe, becoming more rivals because --

THE PRESIDENT: I think the only way that would happen is if it were provoked by greater protectionism, economic protectionism outside the borders of Europe. That is, Europe could get so big and they could integrate the economy of Europe, and they'll have a lot of poor countries coming in -- just like we have poor states and poor regions. If they close their economy, rather than opened it, that could be a difficult thing. But I think it's far more likely that our former enemies will become at least friendlier, if we're not friends; and that all of us together will face the enemies of the nation state in the 21st century.

Q The enemies of the nation state?

THE PRESIDENT: Yes. The organized enemies of the nation state that have vast money and vast access to weapons and technology and travel; the organized crime syndicates; the narco traffickers; the terrorists. And I think the likelihood that all these people will be integrated -- there may be some rogue states that will support them, but I think you're more likely to see the nation states trying to uphold stability in their national lives, increasingly open and democratic -- even China, I think, will become more open and more democratic. They're already electing mayors in a million little towns, literally.

Q In democratic elections?

THE PRESIDENT: Yes. And so I think -- by their standards. They don't have a Republican or a Democratic Party like we do, but they are having these elections. I think in the future the likelihood is that nation states will be allied against the enemies of the organized society, and the open society.

Q Do you expect, then, in the next 10, 20 years to be a terrorist attack in the United States - thinking about the recent events, thinking about the potential for germ warfare, the potential for biological attacks and the potential --

THE PRESIDENT: Oh, absolutely, I think that's a threat.

Q A likelihood?

THE PRESIDENT: Well, I think it's highly likely that someone will try. And keep in mind, the World Trade Center was blown up just a few years ago. We were fortunate to catch the people who did it. Oklahoma City had the terrible explosion.

What I think will happen -- let me back up a minute. I have done everything I could as President to try to organize the permanent government -- the people who will be here when I am gone -- and the Congress to deal with the long-term threat of biological, chemical and

small-scale nuclear war, as well as the increasing sophistication of traditional weapons. And we are doing a massive amount of work now in preparation to try to minimize the chances that it will occur and, God forbid if it should occur, to try to minimize the impact of it. I think, parenthetically, one of the benefits of our research into the human genome is that we'll be able to analyze these viruses much more quickly and come up with antidotes much more quickly than we used to be able to. Even now, when new strains of diseases -- whether it's AIDS or anything else -- comes up, we can identify them so much more quickly than we used to be able to..

So what I think will happen -- let me just make this point -- the organized forces of destruction will take maximum advantage of new technologies and new scientific developments just like democratic societies do. So I think just like the computers are all being miniaturized and people carry these little pads around that have -- and now you've got these gadgets where you can use as a telephone or a typewriter and do e-mail and all that. Well, the same miniaturization will apply to biological and chemical weapons and, if people should get nuclear materials that can be made into a bomb, to nuclear materials -- which is why we've worked so hard with Russia to control access to that stuff.

So we've just got to be ready. There will always be bad guys out there in the world who will try to take advantage of people's vulnerabilities.

Q But aren't the odds against us, when you describe that kind of technological advantage -- I mean, and just recently two people trying -- in separate cases -- trying to get inside America's borders with explosive -- it gets more and more easier to conceal and more and more the likelihood that an American city --

THE PRESIDENT: Well, if you go back through all of human history and you look at conflicts in weapons systems -- and that's what we're talking about, biological, chemical weapons -- offense always precedes defense; that is, you've got to know what you're defending against.

So my goal in this whole thing, trying to mobilize the country on biological, chemical weapons, and make sure the government is doing everything possible, is to close the gap between offense and defense. And the answer to your question is, we won't be -- there might be incidences. I mean, the World Trade Center was blown up; Oklahoma City was blown up. We've got a guy in the laboratory in the middle west almost five years ago who was trying to develop biological agents, political extremist.

Q And there are scary ideas coming out of science, where viruses can attack certain ethnic groups

scary ideas coming out of science, where viruses can attack certain ethnic groups.

THE PRESIDENT: Yes, there are people that --

Q The potential of science to do harm is alarming.

THE PRESIDENT: But, you know, it's always been that way. I mean, it's always been that way. And I think that I'm actually more optimistic than -- keep in mind, no one believes that someone's going to come in and kill everybody in America. That's what we worried about during the Cold War. And we still have to deal with these traditional threats. That's why India and Pakistan is perhaps -- the Kashmiri issue is perhaps the most dangerous one in the world today because you've got

two nuclear power there who are somewhat uncertain about one another and why we have to work hard to avoid that.

But, yes, there will be problems. Yes, there could be terrible incidences. But I would say to the American people, they should, on balance, be hopeful. But what they should do is to support the leadership of this country in putting maximum resources into research and development so that we're prepared. And I think we will grow increasingly sophisticated in picking these people up, increasingly sophisticated in detecting these weapons, and what we can't afford is to have a long period of time where these offensive capabilities of the New Age are better than the defensive capabilities. If we can close the gap between offense and defense we'll be fine.

Q What's interesting about a conversation about the future with you is that because of this office and your curiosity, you see and know more than almost anyone. I mean, you are aware because you talk to the scientists, you talk to people responsible.

THE PRESIDENT: I think about it a lot.

Q You do?

THE PRESIDENT: Sure. I have to. See, I think one of the jobs of the President, because of the unique opportunity of the office you just described, is to always be thinking about what will happen 10, 20, 30 years from now, and to allocate to some time an effort to making decisions for which there will be almost no notice.

You know, right now, I mean, hardly anybody reports on or thinks about the work we're going in biological warfare or chemical warfare -- the speech I gave at the National Science Foundation -- but it's fine. It's what my former National Security Aide, Tony Lake, used to call "the dog that doesn't bark." And there is a sense in which there's a bunch of dogs in this old world you don't want to bark.

Q It's the old notion about if the tree falls in the forest and nobody hears it, did the tree fall. Can you -- are there things that we don't know about that alarm you? This sense of science and where it's at and what's coming down the pike that gives you great pause?

THE PRESIDENT: Well, there are a lot of things that concern me. You know, we've done a lot of work --the other thing that, besides the chemical and biological weapons, trying to protect computer systems.

Q Speak to Y2K. Where are your concerns, and do you think that most of those --

THE PRESIDENT: My concerns -- well, they're much more traditional in Y2K. I think we've done a good job here. We've spent a lot of money -- I say -- we, -- the American people, not just the government, the private sector -- we've spent a lot of money and we've tried to be ready. I feel a high level of confidence. It wouldn't bother me a bit to get on a commercial airline, for example, on New Year's Eve or New Year's Day and fly around. I think our systems are in order here.

My concerns really are for some of our friends around the world that have more rudimentary computer networks and capacities, and whether they will have a shutdown that they won't be able to immediately fix or get around.

Q And make them vulnerable to what?

THE PRESIDENT: Well, if there were problems in the financial

system, what if records disappeared and people lost money? That would be destabilizing in some countries. If power systems --

Q And make them vulnerable to outside forces, to kinds of elements you mentioned earlier?

THE PRESIDENT: Well, maybe, but I think more internal destabilization. What if a power system shuts down in a big country with a hard winter? How long will it take to get back up before anyone would freeze to death? I mean, these are the kinds of practical problems that I'm concerned about.

But I think that -- I'm talking about something far more insidious, though. What we have to -- this is, again, offense and defense. What we have to do -- this technology of computers is changing so fast, and we've got a lot of whizbangs out there, and they can make a ton of money working for bad guys. So what we've got to do is to continuously work on protecting the cyber security, the infrastructure of the information economy, just like we're trying to deal with chemical and biological warfare and the miniaturization of weapons and all this.

But most people are good people. We've got plenty of talented people . We just need to be imagining the future, thinking about all the problems as well as all the opportunities, and then prepare. Society always has problems, there are always misfortunes, but basically, I believe the future is quite promising and far more exciting than any period in history. I wish I were going to live to be 150; I'd love to see what happens.

Q Would you like to be cloned?

THE PRESIDENT: I wouldn't wish that on anybody. (Laughter.)

Q There is this thing, too. I mean, think about Chelsea's children, your grandchildren, say the year 2050, whatever the appropriate time might be. What's this world going to look like? Is it going to be more interesting, more challenging? How will we travel, what kind of food will we eat, will we go to other planets?

THE PRESIDENT: I think we'll be eating food that's like what we eat now. I think it will be safer. I think we'll know a lot more about it, even safer than it is now. I think that in big, urban areas, I think we'll still have our love affairs with cars. I think they will be much more safe. They'll be made of composite materials that are much more resistant to wrecks, and I think where there is a lot of heavy traffic, I think that we'll all travel by a computerized plan.

I also think there will be a lot more rapid rail transit, I think it will be safer, it will be better, and I think we'll be able to do things while we travel and spend more time. I think we will go into outer space, and at sometime in the next century, I think there will be large, permanent platforms sustaining life in outer space that will basically be jumping off places to distant planets and maybe even beyond. That's what I think will happen.

Q Hold on one second. I know you've got to change tape. Okay.

Q You said computerized plan --

THE PRESIDENT: No, I meant cars. You want me to say it again?

Q How much time do we have?

THE PRESIDENT: I just misspoke myself.

Q How much time do we have here?

THE PRESIDENT: I don't know, 10 minutes, five minutes?

You want to do that again?

Q The last question.

Q All right. Okay. Think about the future of your grandchildren, Chelsea's children, the year 2050. What will life be like then? What kind of food, what kind of transportation, will we be living on other planets, will we still be concerned about things that concern us now, like overweight, stuff like that?

THE PRESIDENT: I don't think all of the problems will go away. I think the food will be pretty much like it is now, but even safer. I think that on Earth, we'll travel in automobiles, still, but in traffic jams we'll have automated systems. I think there will be a lot more high-speed rail. I think we'll travel in ways that give us more free time to do things while we travel.

I think that there will be large platforms in outer space that will be jumping off places to distant planets, and I think that the biomedical advances will be stunning. I think a lot of cancers will be cured. I think there will be a vaccine for AIDS. I think that the research in the human gene and the revolution -- the continuing revolution in microchips will enable people to probably cure spinal cord injuries by having a programmed chip that goes into the spine and replicates all the nerves that were damaged.

I think that it will be a fascinating time. And I think there will be lots and lots of continuous daily communication with people across national and cultural lines.

Q Would you go to space if you had the opportunity?

THE PRESIDENT: I might. I'm real interested in it. I like it a lot. I think it's important.

Q What one thing do you most want to accomplish -- I've got to go --when you leave this office? What's the single most important thing for you to accomplish when you leave?

THE PRESIDENT: You mean, after I'm not President anymore?

Q After you're not President.

THE PRESIDENT: I think the most important thing is for me to be a useful citizen of this country and of this world, because I've had opportunities here only my other living predecessors have had. And I think that for me to be able to continue the work I've done in racial and religious and ethnic reconciliation and trying to convince people that we can grow the global economy and still preserve the environment and trying to empower the poor and the dispossessed, in trying to spread the universal impact of education and use technology to benefit ordinary people, these kinds of things -- I think I should continue to do this work and trying -- I want to get young people into public service. I want them to believe this is noble and important work.

So I think in a word, I have to be a good citizen now. That's the most important thing I can do when I leave office is to use the maximum -- to the maximum extent I can, the knowledge that I have, the experience that I've gained to be a really good citizen.

Q Thank you, Mr. President.

THE PRESIDENT: Thank you.

END 5:40 P.M. EST

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release January 22, 1999

REMARKS BY NATIONAL SECURITY ADVISOR SANDY BERGER;
DR. JOSHUA LEDERBERG, NOBEL LAUREATE,
AND JAMIE GORELICK, OF FANNIE MAE FOUNDATION,

ON KEEPING AMERICA SECURE FOR THE 21ST CENTURY

National Academy of Sciences
Washington. D.C.

MR. BERGER: Good morning to all of you and welcome. Let me thank you all for coming. Let me acknowledge in particular Dr. Bruce Alberts, President of the National Academy of Sciences; Dr. William Wulf, President of the National Academy of Engineering; and Dr. Kenneth Shine, President of the National Academy of Medicine.

We are here to discuss emerging threats to America's security as we reach a new century. How do we respond to the threat of terrorists around the world, turning from bullets and bombs to even more insidious and potent weapons? What if they and the rogue states that sponsor them try to attack the critical computer systems that drive our society? What if they seek to use chemical, biological, even nuclear weapons? The United States must deal with these emerging threats now, so that the instruments of prevention develop at least as rapidly as the instruments of disruption.

Today we are confronting these challenges with an extraordinary team of dedicated professionals across our government -- with law enforcement efforts headed by Attorney General Reno and FBI Director Freeh; with strong diplomacy backed by a strong defense under Secretary of State Albright and Secretary of Defense Cohen; with better intelligence under the direction of Director Tenet; and determined efforts to contain weapons proliferation under Energy Secretary Richardson; with emergency management under FEMA Director Witt; private industry cooperation directed by Secretary Daley; and aviation security under Transportation Secretary Slater; and with public health and management and medical research guided by Health and Human Services Secretary Shalala -- who probably did not think she was going to be part of the national security team when she became Secretary of HHS.

And since last spring, with the efforts of the President's National Coordinator for Security Infrastructure Protection and Counterterrorism, Richard Clarke, who is working to make all these pieces fit together in a united effort. And most of all, we have a President who, from the outset of his administration, has put the task of meeting new security threats at the very forefront of our national security strategy -- a President who has driven all of us to seek out the best minds and ask the important questions as we prepare for the future.

Today the President will announce new initiatives to combat these emerging threats. But before the President addresses us, I want to present two important representatives of the private sector. The involvement of the private sector in these efforts, from top researchers at our universities to industry leaders, together with the participation

of state and local governments, is absolutely critical if we are to succeed.

We're pleased to be joined today by Jamie Gorelick, who will discuss the danger that our critical infrastructures are becoming vulnerable to computer and other forms of attack, the cyber threat. She is Vice Chair of Fannie Mae, the nation's largest funder for home mortgages. She is also the former co-chair of the Advisory Committee of the President's Commission on Critical Infrastructure Protection. And we in the administration know her well from her extraordinarily able tenure as Deputy Attorney General and General Counsel of the Department of Defense.

But first we will hear from Dr. Joshua Lederberg, a geneticist and President Emeritus of the Rockefeller University in New York. Dr. Lederberg won the Nobel Prize in Medicine at age 33 -- which, I suppose, not only makes me a failure -- (laughter) -- but only gives my children a few years. (Laughter.) At least the President can say that he was governor by the time he was 33. (Laughter and applause.)

Dr. Lederberg has been a frequent advisor to our government on the threat of biological weapons, and he was a key participant in a roundtable on this issue that the President convened last spring.

Dr. Lederberg. (Applause.)

DR. LEDERBERG: Mr. President, distinguished officers of government, scientific colleagues, ladies and gentlemen. For over half a century I've had the joy and excitement of research on the microbial world, its evolution, the conspiracies it harbors, and its ambiguous competition with the human species.

There have been many occasions in this very hall to share news of profound scientific discoveries which not only broaden our conceptual understanding of ourselves and our biological extended family in the living world, but gave us ever sharper tools to deal with pestilence and decay.

But throughout that time, I've been imbued with the fear that, just as happened with physics and chemistry, that great advances in medicine would be turned into engines of war. That fear has been compounded by the deterioration of civil order that might otherwise restrain the use of weapons of mass destruction, and by the ease with which nature already provides the germs of disease that might be used as weapons.

In fact, the very triumph of the democratic world's military technology with guided missiles and dominance of the battlefield drives the agents of disorder to ever more subversive means of attack and inspires new scales of terrorism, grand and small.

We have made great progress, diplomatically and in international law, with the prohibitions against biological and chemical weapons, though there is some way to go in their enforcement. However, our civilian populations have, until now, been almost undefended against bioterrorism, in an era where political disorder weakens the system of deterrence that had been our main shield throughout the Cold War.

The reconstruction of bio-defenses must be regarded as a branch of public health and it is equally necessary to deal with cyclic renewals of historic national plagues as much as with those borne of malice.

So it has been extremely gratifying that during the past months and year these concerns, voiced so persuasively by many of my colleagues

here at the Academy and the Institute of Medicine, have reached the attention of the highest levels of government, and action plans have been embodied in numerous executive orders and in the budgetary proposals that the President will discuss this morning.

Thank you, and here's Jamie Gorelick. (Applause.)

MS. GORELICK: Mr. President, distinguished guests. Ten years ago I would not have put cyber terrorism at the top of the threats to our national security. But the landscape has changed. Given how well-armed we are, as Josh said, as a nation, but how reliant we are on computers in our everyday business and private lives, our nation's cyber systems become a tremendous target.

Today a small group of technically sophisticated people with nothing more than off-the-shelf computer equipment can get into, can disrupt the computers and the Internet connections on which our finance, telecommunications, power, water systems, emergency service systems all depend.

Is this speculation? No, it is not. In exercise eligible receiver, our Defense Department conducted a war game using this technique and came to just that conclusion. And terrorists, organized crime, drug cartels, as well as nation states are either creating cybertech capabilities or are talking about using them. I believe that cyberspace is the next battlefield for this nation.

Now, cyber terrorism may be a new issue to many Americans, but it's not new to me and it's not new to this administration. In 1995, our Attorney General asked me to chair a critical infrastructure working group that brought together Justice and Defense and the intelligence community to begin to address what we saw as a new and emerging threat. The President then appointed a commission on critical infrastructure protection whose advisory board I co-chaired.

In response to his commission's work, last year the President signed two directives -- to strengthen U.S. readiness to meet unconventional threats to our nation, and to protect our critical infrastructures. He appointed a national coordinator, Dick Clarke, to review and handle and coordinate security infrastructure protection and counterterrorism, and a national plan is under development to ensure that America can defend itself in cyberspace.

Now, as part of that national plan I hope that we can see action in a number of areas, three of which I see as particularly pressing. The first, both the public and private sectors need to be aware of the problem and the security measures that can be taken to address it. I'd like to see the private sector work with the federal government to make sure that we have enough people who are trained in computer security, which we do not now have.

Second, we need to encourage ways for the government and the private sector to share information on cyber intrusions and on new techniques for preventing those intrusions, and responding to them. A government-chartered, privately-run center could do this, and also help develop standards for use in both industry and government. This will complement the government's obligation to ensure that we have the ability to respond as a nation to any attack.

Third, the companies that manage and assess risk for private sector clients, like insurance companies and accounting firms, need to focus on the risk that American businesses face from cyber attacks. I'd like to see the widespread use of cyber security best practices and standards as a tool of good business management for every business.

I want to thank the President for his appreciation of the threat and his commitment of resources to address it. And I will urge the business community to respond in kind. This President has always been sensitive to the promise of the Information Age, what it can mean to students, what it can mean to families, to a world drawn closer in many ways by the speed of communication. At the same time, he knows that that promise comes with a price, and the price is vigilance, because so much is at stake.

We're grateful for his leadership both in promoting the cyber world and in protecting it.

Ladies and gentlemen, it is my honor and my personal privilege to present to you the President of the United States. (Applause.)

END

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release October 22, 1997

Critical Foundations Thinking Differently

"Our responsibility is to build the world of tomorrow by embarking on a period of construction -- one based on current realities but enduring American values and interests..."

President William J. Clinton
National Security Strategy

Introduction

The United States is in the midst of a tremendous cultural change -- a change that affects every aspect of our lives. The cyber dimension promotes accelerating reliance on our infrastructures and offers access to them from all over the world, blurring traditional boundaries and jurisdictions. National defense is not just about government anymore, and economic security is not just about business. The critical infrastructures are central to our national defense and our economic power, and we must lay the foundations for their future security on a new form of cooperation between the private sector and the federal government.

The federal government has an important role to play in defense against cyber threats -- collecting information about tools that can do harm, conducting research into defensive technologies, and sharing defensive techniques and best practices. Government also must lead and energize its own protection efforts, and engage the private sector by offering expertise to facilitate protection of privately owned infrastructures.

In the private sector, the defenses and responsibilities naturally encouraged and expected as prudent business practice for owners and operators of our infrastructures are the very same measures needed to protect against the cyber tools available to terrorists and other threats to national security.

Venues for Change

Terrorist bombings of US forces in Saudi Arabia, the World Trade Center in New York City, and the federal building in Oklahoma City remind us that the end of the Cold War has not eliminated threats of hostile action against the United States.

In recognition of comparable threats to our national infrastructures, President Clinton signed Executive Order 13010 on July 15, 1996, establishing the President's Commission on Critical Infrastructure Protection. The Commission was chartered to conduct a comprehensive review and recommend a national policy for protecting critical infrastructures and assuring their continued operation.

Our Process -- Who We Are and What We Did
Composition and Operation of the Commission

This was an unusually large commission with broad representation from federal departments and agencies and from the private sector. An Advisory Committee of industry leaders appointed by the President provided the perspective of the infrastructure owners and operators. A Steering Committee, composed of the Commission's Chairman and four top government officials, oversaw the Commission's work on behalf of the Principals Committee, which included Cabinet Officers, heads of agencies, and senior White House staff members. The Commission generally operated by consensus. Every recommendation was discussed at length with the full Commission and most were revised several times before final approval. No Commissioner agreed completely with all of the recommendations. Nevertheless, each accepted the final report as a reasonable and balanced recommendation to the President.

Sector Studies

The Commission divided its work into five sectors based on the common characteristics of the included industries. The sectors are:

Information and Communications
Banking and Finance
Energy, Including Electrical Power, Oil and Gas
Physical Distribution
Vital Human Services

The Commission characterized the sectors, studied their vulnerabilities, and looked for solutions.

We prepared comprehensive working papers for each of the five sectors providing specific recommendations. Other work contains the results of deliberations on issues that are not sector specific. Among them is a paper on Research and Development Recommendations, which outlines a comprehensive set of topics regarding the long term needs of infrastructure protection. The paper on National Structures contains our conclusions and recommendations about the functions and responsibilities for infrastructure assurance and the creation of new units in the federal government and the private sector, and some that are jointly staffed by government employees and representatives of the infrastructure owners and operators. The paper on Shared Infrastructures: Shared Threats is our collected analysis of the vulnerabilities and threats facing the critical infrastructures.

We recognize the enormous significance of physical threats, but we have a significant amount of experience in dealing with them. It is the cyber threat that is new. Cyber issues dominate this analysis because networked information systems present fundamentally new security challenges.

Public Hearings and Outreach

We conducted extensive meetings with a range of professional and trade associations concerned with the infrastructures, private sector infrastructure users and providers, academia, different state and local government agencies, consumers, federal agencies, and numerous others. Of special interest were five public meetings in major cities.

We attended dozens of conferences and roundtables with a variety of groups, and we arranged two strategic simulations with participants drawn from across the infrastructures and from all levels of government. We encouraged questions and comments by anyone, and established a World Wide Web site to facilitate contact. Several

meetings with Congressional Members and their staffs added a very useful perspective to our research.

Development of our Critical Issues

During the preparation of the sector papers we identified several dozen issues for which recommendations might be appropriate. Each issue was described, relevant observations, findings, and conclusions were collected, and several alternative recommendations were prepared. The Commission then deliberated each issue and selected one of the alternative recommendations.

We Found Increasing Dependence on Critical Infrastructures

The development of the computer and its astonishingly rapid improvements have ushered in the Information Age that affects almost all aspects of American commerce and society. Our security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers.

Increasing Vulnerabilities

Classical physical disruptions. A satchel of dynamite or a truckload of fertilizer and diesel fuel have been frequent terrorist tools. The explosion and the damage are so certain to draw attention that these kinds of attacks continue to be among the probable threats to our infrastructures.

New, cyber threats. Today, the right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives, and the perpetrator would be harder to identify and apprehend.

The rapid growth of a computer-literate population ensures that increasing millions of people possess the skills necessary to consider such an attack. The wide adoption of public protocols for system interconnection and the availability of hacker tool libraries make their task easier. While the resources needed to conduct a physical attack have not changed much recently, the resources necessary to conduct a cyber attack are now commonplace. A personal computer and a simple telephone connection to an Internet Service Provider anywhere in the world are enough to cause a great deal of harm.

System complexities and interdependencies. The energy and communications infrastructures especially are growing in complexity and operating closer to their designed capacity. This creates an increased possibility of cascading effects that begin with a rather minor and routine disturbance and end only after a large regional outage. Because of their technical complexity, some of these dependencies may be unrecognized until a major failure occurs.

A Wide Spectrum of Threats

Of the many people with the necessary skills and resources, some may have the motivation to cause substantial disruption in services or destruction of the equipment used to provide the service.

This list of the kinds of threats we considered shows the scope of activity with potentially adverse consequences for the infrastructures, and the diversity of people who might engage in that activity. It may

not be possible to categorize the threat until the perpetrator is identified -- for example, we may not be able to distinguish industrial espionage from national intelligence collection.

Natural events and accidents. Storm-driven wind and water regularly cause service outages, but the effects are well known, the providers are experienced in dealing with these situations, and the effects are limited in time and geography.

Accidental physical damage to facilities is known to cause a large fraction of system incidents. Common examples are fires and floods at central facilities and the ubiquitous back-hoe that unintentionally severs pipes or cables.

Blunders, errors, and omissions. By most accounts, incompetent, inquisitive, or unintentional human actions (or omissions) cause a large fraction of the system incidents that are not explained by natural events and accidents. Since these usually only affect local areas, service is quickly restored; but there is potential for a nationally significant event.

Insiders. Normal operation demands that a large number of people have authorized access to the facilities or to the associated information and communications systems. If motivated by a perception of unfair treatment by management, or if suborned by an outsider, an insider could use authorized access for unauthorized disruptive purposes.

Recreational hackers. For an unknown number of people, gaining unauthorized electronic access to information and communication systems is a most fascinating and challenging game. Often they deliberately arrange for their activities to be noticed even while hiding their specific identities. While their motivations do not include actual disruption of service, the tools and techniques they perfect among their community are available to those with hostile intent.

Criminal activity. Some are interested in personal financial gain through manipulation of financial or credit accounts or stealing services. In contrast to some hackers, these criminals typically hope their activities will never be noticed, much less attributed to them. Organized crime groups may be interested in direct financial gain, or in covering their activity in other areas.

Industrial espionage. Some firms can find reasons to discover the proprietary activities of their competitors, by open means if possible or by criminal means if necessary. Often these are international activities conducted on a global scale.

Terrorism. A variety of groups around the world would like to influence US policy and are willing to use disruptive tactics if they think that will help.

National intelligence. Most, if not all, nations have at least some interest in discovering what would otherwise be secrets of other nations for a variety of economic, political, or military purposes.

Information warfare. Both physical and cyber attacks on our infrastructures could be part of a broad, orchestrated attempt to disrupt a major US military operation or a significant economic activity.

Lack of Awareness

We have observed that the general public seems unaware of the extent of the vulnerabilities in the services that we all take for granted, and that within government and among industry decision-makers, awareness is limited. Several have told us that there has not yet been a cause for concern sufficient to demand action.

We do acknowledge that this situation seems to be changing for the better. The public news media seem to be carrying relevant articles more frequently; attendance at conferences of security professionals is up; and vendors are actively introducing new security products.

The Commission believes that the actions recommended in this report will increase sensitivity to these problems, and reduce our vulnerabilities at all levels.

No National Focus

Related to the lack of awareness is the need for a national focus or advocate for infrastructure protection. Following up on our report to the President, we need to build a framework of effective deterrence and prevention. This is not simply the usual study group's lament that no one is in charge. These infrastructures are so varied, and form such a large part of this nation's economic activity, that no one person ororganization can be in charge. We do not need, and probably could not stand, the appointment of a Director of Infrastructures. We do need, and recommend, several more modest ways to create and maintain a national focus on the issues.

Protection of our infrastructures will not be accomplished by a big federal project. It will require continuous attention and incremental improvement for the foreseeable future.

We Concluded

Life on the information superhighway isn't much different from life on the streets; the good guys have to hustle to keep the bad guys from getting ahead.

Rules Change in Cyberspace -- New Thinking is Required

It is not surprising that infrastructures have always been attractive targets for those who would do us harm. In the past we have been protected from hostile attacks on the infrastructures by broad oceans and friendly neighbors. Today, the evolution of cyber threats has changed the situation dramatically. In cyberspace, national borders are no longer relevant. Electrons don't stop to show passports.

Potentially serious cyber attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker.

Formulas that carefully divide responsibility between foreign defense and domestic law enforcement no longer apply as clearly as they used to. With the existing rules, you may have to solve the crime before you can decide who has the authority to investigate it. Senator Sam Nunn, remarks to the PCCIP Advisory Committee, Washington, DC, September 7, 1997.

We Should Act Now to Protect our Future

The Commission has not discovered an imminent attack or a credible threat sufficient to warrant a sense of immediate national crisis. However, we are quite convinced that our vulnerabilities are increasing steadily while the costs associated with an effective attack continue to drop. What is more, the investments required to improve the situation are still relatively modest, but will rise if we procrastinate.

We should attend to our critical foundations before the storm arrives, not after: waiting for disaster will prove as expensive as it is irresponsible.

Infrastructure Assurance is a Shared Responsibility

National security requires much more than military strength. Our world position, our ability to influence others, our standard of living, and our own self-image depend on economic prosperity and public confidence. Clear distinctions between foreign and domestic policy no longer serve our interests well.

At the same time, the effective operation of our military forces depends more and more on the continuous availability of infrastructures, especially communications and transportation, that are not dedicated to military use. While no nation state is likely to attack our territory or our armed forces, we are inevitably the target of ill-will and hostility from some quarters. Disruption of the services on which our economy and well-being depend could have significant effects, and if repeated frequently could seriously harm public confidence. Because our military and private infrastructures are becoming less and less separate, because the threats are harder to differentiate as from local criminals or foreign powers, and because the techniques of protection, mitigation, and restoration are largely the same, we conclude that responsibility for infrastructure protection and assurance can no longer be delegated on the basis of who the attacker is or where the attack originates. Rather, the responsibility should be shared cooperatively among all of the players.

We Recommend A Broad Program of Awareness and Education

Because of our finding that the public in general and many industry and government leaders are insufficiently aware of the vulnerabilities, we have recommended a broad and continuous program of awareness and education to cover all possible audiences. We include White House conferences, National Academy studies, presentations at industry associations and professional societies, development and promulgation of elementary and secondary curricula, and sponsorship of graduate studies and programs.

Infrastructure Protection through Industry Cooperation and Information Sharing

We believe the quickest and most effective way to achieve a much higher level of protection from cyber threats is to raise the level of existing protection through application of best practices. We have accordingly recommended a sector-by-sector cooperation and information sharing strategy. In general, these sector structures should be partnerships among the owners and operators, and appropriate

government agencies, which will identify and communicate best practices. We have especially asked the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to provide technical skills and expertise required to identify and evaluate vulnerabilities in the associated information networks and control systems.

One very effective practice is a quantitative risk-management process, addressing physical attacks, cyber attacks that could corrupt essential information or deny service, the possibility of cascading effects, and new levels of interdependency.

The first focus of sector cooperation should be to share information and techniques related to risk management assessments. This should include development and deployment of ways to prevent attacks, mitigate damage, quickly recover services, and eventually reconstitute the infrastructure.

We suggest consideration of these immediate actions prior to the completion of a formal risk assessment: (1) Isolate critical control systems from insecure networks by disconnection or adequate firewalls; (2) Adopt best practices for password control and protection, or install more modern authentication mechanisms; (3) Provide for individual accountability through protected action logs or the equivalent.

The sector cooperation and information sharing needed to improve risk assessments and to protect against probable attacks may naturally develop into sharing of information on current status. This would permit assessing whether one of the infrastructures is under a coordinated attack -- physical, cyber, or combined. As this process develops, the national center for analysis of such information should be in place and ready to cooperate.

Reconsideration of Laws Related to Infrastructure Protection

Law has failed to keep pace with technology. Some laws capable of promoting assurance are not as clear or effective as they could be. Still others can operate in ways that may be unfriendly to security concerns. Sorting them all out will be a lengthy and massive undertaking, involving efforts at local, state, federal, and international levels. Recognizing the dynamic nature of legal reform, we attempted to lay a foundation through various studies, papers, and a legal authorities database that can aid eventual implementation of our recommendations and assist owners, operators, and government at all levels.

We also offered a number of preliminary legal recommendations intended to jump-start this process of reform. We identified existing laws that could help the government take the lead and serve as a model of standards and practices for the private sector. We identified other areas of law which, with careful attention, can enable infrastructure owners and operators to take precautions proportionate to the threat. We identified still other areas of law that should be molded to enable a greater degree of government-industry partnership in areas such as information sharing.

A Revised Program of Research and Development

The Commission believes that some of the basic technology needed to improve infrastructure protection already exists, but needs to be widely deployed. In other areas, additional research effort is needed.

At the same time the Commission recognizes that we are not now able to deploy several capabilities that we need. We have, therefore, recommended a program of research and development focused on those future capabilities. Among them are new capabilities for detection and identification of intrusion and improved simulation and modeling capability to understand the effects of interconnected and fully interdependent infrastructures.

A National Organization Structure

In order to be effective, recommendations must discuss not only what is to be done, but how it will get done and who will do it. We have recommended the following partnering organizations be established to be responsible for specific parts of our vision:

Sector Coordinators to provide the focus for industry cooperation and information sharing, and to represent the sector in matters of national cooperation and policy;

Lead Agencies, designated within the federal government, to serve as a conduit from the government into each sector and to facilitate the creation of sector coordinators, if needed;

National Infrastructure Assurance Council of industry CEOs. Cabinet Secretaries, and representatives of state and local government to provide policy advice and implementation commitment;

Information Sharing and Analysis Center to begin the step-by-step process of establishing a realistic understanding of what is going on in our infrastructures - of distinguishing actual attack from coincidental events. Infrastructure Assurance Support Office to house the bulk of the national staff which is responsible for continuous management and follow-through of our recommendations; and

Office of National Infrastructure Assurance as the top-level policy making office connected closely to the National Security Council and the National Economic Council.

Conclusion

It is clear to us that infrastructure assurance must be a high priority for the nation in the Information Age. With escalating dependence on information and telecommunications, our infrastructures no longer enjoy the protection of oceans and military forces. They are vulnerable in new ways. We must protect them in new ways. And that is what we recommend in this report.

The public and private sector share responsibility for infrastructure protection. Our recommendations seek to provide structures for the partnership needed to assure our future security. Further, they seek to define new ways for approaching infrastructure assurance -- ways that recognize the new thinking required in the Information Age, the new international security environment emerging from our victory in the Cold War and both the promise and danger of technology moving at breakneck speed.

We do not so much offer solutions as directions -- compass headings that will help navigate through a new geography and ensure the continuity of the infrastructures that underpin America's economic, military, and social strength.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release January 22, 1999

REMARKS BY THE PRESIDENT
ON KEEPING AMERICA SECURE FOR THE 21ST CENTURY

National Academy of Sciences
Washington, D.C.

10:30 A.M. EST

THE PRESIDENT: Thank you very much. Jamie, Dr. Lederberg, I'd like to thank you for your service in this and so many other ways. I would like to thank Sandy Berger for many things, including indulging my nagging on this subject for the better part of six years now.

I was so relieved that Dr. Lederberg not very long ago -- well, last year -- brought a distinguished panel of experts together to discuss this bioterrorism threat, because I then had experts to cite on my concern and nobody thought I was just reading too many novels late at night. (Laughter.)

Madame Attorney General, Secretary Shalala, Secretary Richardson, Director Witt, Deputy Secretary Hamre, Commandant of the Coast Guard and our other military leaders who are here, Mr. Clarke, ladies and gentlemen. I'm delighted to be here to discuss this subject. With some trepidation, Sandy Berger noted that Dr. Lederberg won a Nobel Prize at 33, and I was governor -- you can infer from that that I was not very good at chemistry and biology. (Laughter.)

But any democracy is imbued with the responsibility of ordinary citizens who do not have extraordinary expertise to meet the challenges of each new age. And that is what we are all trying to do. Our country has always met the challenges of those who would do us harm. At the heart of our national defense I have always believed is our attempt to live by our values -- democracy, freedom, equal opportunity. We are working hard to fulfill these values at home. And we are working with

nations around the world to advance them, to build a new era of interdependence where nations work together -- not simply for peace and security, but also for better schools and health care, broader prosperity, a cleaner environment and a greater involvement by citizens everywhere in shaping their own future.

In the struggle to defend our people and values and to advance them wherever possible, we confront threats both old and new -- open borders and revolutions in technology have spread the message and the gifts of freedom but have also given new opportunities to freedom's enemies. Scientific advances have opened the possibility of longer, better lives. They have also given the enemies of freedom new opportunities.

Last August, at Andrews Air Force Base, I grieved with the families of the brave Americans who lost their lives at our embassy in Kenya. They were in Africa to promote the values America shares with friends of freedom everywhere -- and for that they were murdered by terrorists. So, too, were men and women in Oklahoma City, at the World Trade Center, Khobar Towers, on Pan Am 103.

The United States has mounted an aggressive response to terrorism -- tightening security for our diplomats, our troops, our air travelers, improving our ability to track terrorist activity, enhancing cooperation with other countries, strengthening sanctions on nations that support terrorists.

Since 1993, we have tripled funding for FBI anti-terrorist efforts. Our agents and prosecutors, with excellent support from our intelligence agencies, have done extraordinary work in tracking down perpetrators of terrorist acts and bringing them to justice. And as our air strikes against Afghanistan -- or against the terrorist camps in Afghanistan -- last summer showed, we are prepared to use military force against terrorists who harm our citizens. But all of you know the fight against terrorism is far from over. And now, terrorists seek new tools of destruction.

Last May, at the Naval Academy commencement, I said terrorist and outlaw states are extending the world's fields of battle, from physical space to cyberspace, from our earth's vast bodies of water to the complex workings of our own human bodies. The enemies of peace realize they cannot defeat us with traditional military means. So they are working on two new forms of assault, which you've heard about today: cyber attacks on our critical computer systems, and attacks with weapons of

mass destruction -- chemical, biological, potentially even nuclear weapons. We must be ready -- ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire and health services -- or military assets.

More and more, these critical systems are driven by, and linked together with, computers, making them more vulnerable to disruption. Last spring, we saw the enormous impact of a single failed electronic link, when a satellite malfunctioned -- disabled pagers, ATMs, credit card systems and television networks all around the world. And we already are seeing the first wave of deliberate cyber attacks -- hackers break into government and business computers, stealing and destroying information, raiding bank accounts, running up credit card charges, extorting money by threats to unleash computer viruses.

The potential for harm is clear. Earlier this month, an ice storm in this area crippled power systems, plunging whole communities into darkness and disrupting daily lives. We have to be ready for adversaries to launch attacks that could paralyze utilities and services across entire regions. We must be ready if adversaries seek to attack with weapons of mass destruction, as well. Armed with these weapons, which can be compact and inexpensive, a small band of terrorists could inflict tremendous harm.

Four years ago, though, the world received a wake-up call when a group unleashed a deadly chemical weapon, nerve gas, in the Tokyo subway. We have to be ready for the possibility that such a group will obtain biological weapons. We have to be ready to detect and address a biological attack promptly, before the disease spreads. If we prepare to defend against these emerging threats we will show terrorists that assaults on America will accomplish nothing but their own downfall.

Let me say first what we have done so far to meet this challenge. We've been working to create and strengthen the agreement to keep nations from acquiring weapons of mass destruction, because this can help keep these weapons away from terrorists, as well. We're working to ensure the effective implementation of the Chemical Weapons Convention; to obtain an accord that will strengthen compliance with the biological weapons convention; to end production of nuclear weapons material. We must ratify the Comprehensive Test Ban Treaty to end nuclear tests once and for all.

As I proposed Tuesday in the State of the Union Address, we should substantially increase our efforts to help Russia and other former Soviet nations prevent weapons material and knowledge from falling into the hands of terrorists and outlaw states. In no small measure we should do this by continuing to expand our cooperative work with the thousands of Russian scientists who can be used to advance the causes of world peace and health and well-being, but who if they are not paid, remain a fertile field for the designs of terrorists.

But we cannot rely solely on our efforts to keep weapons from spreading. We have to be ready to act if they do spread. Last year, I obtained from Congress a 39 percent budget increase for chemical and biological weapons preparedness. This is helping to accelerate our ongoing effort to train and equip fire, police and public health personnel all across our country to deal with chemical and biological emergencies. It is helping us to ready armed forces and National Guard units in every region to meet this challenge; and to improve our capacity to detect an outbreak of disease and save lives; to create the first ever civilian stockpile of medicines to treat people exposed to biological and chemical hazards; to increase research and development on new medicines and vaccines to deal with new threats.

Our commitment to give local communities the necessary tools already goes beyond paper and plans. For example, parked just outside this building is a newly designed truck we have provided to the Arlington, Virginia, Fire Department. It can rapidly assist and prevent harm to people exposed to chemical and biological dangers.

But our commitment on the cyber front has been strong, as well. We've created special offices within the FBI and the Commerce Department to protect critical systems against cyber attack. We're building partnerships with the private sector to find and reduce vulnerabilities; to improve warning systems; to rapidly recover if attacks occur. We have an outstanding public servant in Richard Clarke, who is coordinating all these efforts across our government.

Today, I want to announce the new initiatives we will take, to take us to the next level in preparing for these emerging threats. In my budget, I will ask Congress for $10 billion to address terrorism and terrorist-emerging tools. This will include nearly $1.4 billion to protect citizens against chemical

and biological terror -- more than double what we spent on such programs only two years ago.

We will speed and broaden our efforts, creating new local emergency medical teams, employing in the field portable detection units the size of a shoe box to rapidly identify hazards; tying regional laboratories together for prompt analysis of biological threats. We will greatly accelerate research and development, centered in the Department of Health and Human Services, for new vaccines, medicines and diagnostic tools.

I should say here that I know everybody in this crowd understands this, but everyone in America must understand this: the government has got to fund this. There is no market for the kinds of things we need to develop; and if we are successful, there never will be a market for them. But we have got to do our best to develop them. These cutting-edge efforts will address not only the threat of weapons of mass destruction, but also the equally serious danger of emerging infectious diseases. So we will benefit even if we are successful in avoiding these attacks.

The budget proposal will also include $1.46 billion to protect critical systems from cyber and other attacks. That's 40 percent more than we were spending two years ago. Among other things, it will help to fund four new initiatives. First, an intensive research effort to detect intruders trying to break into critical computer systems. Second, crime -- excuse me -- detection networks, first for our Defense Department, and later for other key agencies so when one critical computer system is invaded, others will be alerted instantly. And we will urge the private sector to create similar structures.

Third, the creation of information centers in the private sector so that our industries can work together and with government to address cyber threats. Finally, we'll ask for funding to bolster the government's ranks of highly skilled computer experts -- people capable of preventing and responding to computer crises.

To implement this proposal, the Cyber Corps program, we will encourage federal agencies to train and retrain computer specialists, as well as recruiting gifted young people out of college.

In all our battles, we will be aggressive. At the same time I want you to know that we will remain committed to uphold privacy rights and other constitutional protections, as well as the proprietary rights of American businesses. It is essential that we do not undermine liberty in the name of liberty. We can prevail over terrorism by drawing on the very best in our free society -- the skill and courage of our troops, the genius of our scientists and engineers, the strength of our factory workers, the determination and talents of our public servants, the vision of leaders in every vital sector.

I have tried as hard as I can to create the right frame of mind in America for dealing with this. For too long the problem has been that not enough has been done to recognize the threat and deal with it. And we in government, frankly, weren't as well organized as we should have been for too long. I do not want the pendulum to swing the other way now, and for people to believe that every incident they read about in a novel or every incident they see in a thrilling movie is about to happen to them within the next 24 hours.

What we are seeing here, as any military person in the audience can tell you, is nothing more than a repetition of weapons systems that goes back to the beginning of time. An offensive weapons system is developed, and it takes time to develop the defense. And then another offensive weapon is developed that overcomes that defense, and then another defense is built up -- as surely as castles and moats held off people with spears and bows and arrows and riding horses, and the catapult was developed to overcome the castle and the moat.

But because of the speed with which change is occurring in our society -- in computing technology, and particularly in the biological sciences -- we have got to do everything we can to make sure that we close the gap between offense and defense to nothing, if possible. That is the challenge here.

We are doing everything we can, in ways that I can and in ways that I cannot discuss, to try to stop people who would misuse chemical and biological capacity from getting that capacity. This is not a cause for panic -- it is a cause for serious, deliberate, disciplined, long-term concern. And I am absolutely convinced that if we maintain our clear purpose and our strength of will, we will prevail here. And thanks to so many of you in this audience, and your colleagues throughout the United States, and like-minded people throughout the world, we

have better than a good chance of success. But we must be deliberate, and we must be aggressive.

Thank you very much. (Applause.)

END

10:45 A.M. EST

CRITICAL INFRASTRUCTURE ASSURANCE OFFICE

The President's Remarks at the Naval Academy

The signing of Presidential Decision Directives 62 and 63 was announced by President William J. Clinton on May 22, 1998 in his remarks to the graduating class at the United States Naval Academy in Annapolis, Maryland. The text of the President's address was subsequently released by the White House. We have mirrored the transcript of his speech here at the CIAO Web site to facilitate access to information about these Administration initiatives.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release May 22, 1998

REMARKS BY THE PRESIDENT AT THE UNITED STATES NAVAL ACADEMY COMMENCEMENT

United States Naval Academy -- Annapolis, Maryland

10:22 A.M. EDT

THE PRESIDENT: Thank you very much. *(Applause.)* Thank you. Thank you very much. Secretary Dalton, thank you for your generous introduction and your dedicated service. Admiral Larson, thank you. Admiral Johnson, General Krulak, Admiral Ryan -- Visitor's Chair Byron; to the faculty and staff of the Academy; distinguished guests; to proud parents and family members, and especially to the Brigade of Midshipmen: I am honored to be here today. And pursuant to longstanding tradition, I bring with me a small gift. I hereby free all midshipmen who are on restriction for minor conduct offenses. *(Applause.)*

There was so much enthusiasm, I wonder if you heard the word, "minor" offenses. *(Laughter.)*

You know, the President has the signal honor of addressing all of our service academies serially -- one after the other in appropriate order. This is the second time I have had the great honor of being here at the Naval Academy. But I began to worry about my sense of timing. I mean, what can you say to graduating midshipmen in a year when the most famous ship on Earth is again the Titanic? *(Laughter.)* But then I learned this is a totally, almost blindly, confident bunch. After all, over in King Hall you eat cannonballs. *(Laughter.)* Now, for those of you who don't know what they are, they're not the ones Francis Scott Key saw flying over Fort McHenry, they're just huge apple dumplings. Nonetheless, they require a lot of confidence. *(Laughter.)*

I will try to be relatively brief today. I was given only one instruction -- I should not take as long as your class took to scale Herndon Monument. (Applause.) Now, at four hours and five minutes -- *(applause)* -- the slowest time in recorded history -- *(applause)* -- I have a lot of leeway. *(Laughter.)*

But you have more than made up for it. You have done great things -- succeeding in a rigorous academic environment, trained to be superb officers. You have done extraordinary volunteer work, for which I am personally very grateful. In basketball, you made it to the NCAAs for the second time in a row. *(Applause.)* You defeated Army in football last fall. *(Applause.)* In fact, you were 26-6 against teams from Army this year. And while I remain neutral in these things -- *(laughter)* -- I salute your accomplishments. *(Laughter.)*

Let me also join the remarks that Secretary Dalton in congratulating your Superintendent. Admiral Larson has performed remarkable service as an aviator, submarine commander, Commander-in-Chief in the Pacific, twice at the helm of the Academy. I got to know him well when he was our Commander-in-Chief in the Pacific. I came to appreciate more than I otherwise ever could have his unique blend of intelligence and insight and character, and passionate devotion to duty.

In view of the incident on the Indian subcontinent in the last few days, I think it's important for the historical record to note that the first senior official of the United States who told me that there was a serious potential problem there and we had better get ready for it was Admiral Chuck Larson, several years ago. *(Applause.)*

When I asked him to return to the Academy, I thought it was almost too much, and then I realized it might have been too little, for he loves this Academy so much this is hardly tough duty. He met all its challenges. He taught you midshipmen to strive for excellence without arrogance, to maintain the highest ethical standards.

Admiral, on behalf of the American people, I thank you for your service here, your 40 years in the Navy, your devotion to the United States. We are all very grateful to you. *(Applause.)*

I also have every confidence that Admiral Ryan is a worthy successor, and I wish him well.

As I speak to you and other graduates this spring, I want to ask you to think about the challenges we face as a nation in the century that is just upon us, and how our mission must be to adapt to the changes of changing times while holding fast to our enduring ideals. In the coming weeks, I will talk about how the information revolution can widen the circle of opportunity or deepen inequality; about how immigration and our nation's growing diversity can strengthen and unite America, or weaken and divide it.

But nothing I will have the chance to talk about this spring is more important than the mission I charge you with today -- the timeless mission of our men and women in uniform: protecting our nation and upholding our values in the face of the changing threats that are as new as the new century.

Members of the Class of 1998, you leave the Yard at the dawn of a new millennium, in a time of great hope. Around the world people are embracing peace, freedom, free markets. More and more nations are

President Clinton Describes the Threats and Challenges Created by Cyberspace

committed to educating all their children and stopping the destruction of our environment. The information revolution is sparking economic growth and spreading the ideas of freedom around the world. Technology is moving so fast today that the top-of-the-line, high-speed computers you received as Plebes today are virtually museum pieces. *(Laughter.)*

In this world, our country is blessed with peace, prosperity, declining social ills. But today's possibilities are not tomorrow's guarantees.

Just last week, India conducted a series of nuclear explosive tests, reminding us that technology is not always a force for good. India's action threatens the stability of Asia and challenges the firm international consensus to stop all nuclear testing. So again I ask India to halt its nuclear weapons program and join the 149 other nations that have already signed the Comprehensive Test Ban Treaty. And I ask Pakistan to exercise restraint, to avoid a perilous nuclear arms race.

This specter of a dangerous rivalry in South Asia is but one of the many signs that we must remain strong and vigilant against the kinds of threats we have seen already throughout the 20th century -- regional aggression and competition, bloody civil wars, efforts to overthrow democracies.

But also, our security is challenged increasingly by non-traditional threats, from adversaries both old and new -- not only hostile regimes, but also terrorists and international criminals, who cannot defeat us in traditional theaters of battle, but search instead for new ways to attack, by exploiting new technologies and the world's increasing openness.

As we approach the 21st century, our foes have extended the fields of battle -- from physical space to cyberspace; from the world's vast bodies of water to the complex workings of our own human bodies. Rather than invading our beaches or launching bombers, these adversaries may attempt cyberattacks against our critical military systems and our economic base. Or they may deploy compact and relatively cheap weapons of mass destruction -- not just nuclear, but also chemical or biological, to use disease as a weapon of war. Sometimes the terrorists and criminals act alone. But increasingly, they are interconnected, and sometimes supported by hostile countries.

If our children are to grow up safe and free, we must approach these new 21st century threats with the same rigor and determination we applied to the toughest security challenges of this century. We are taking strong steps against these threats today. We've improved antiterrorism cooperation with other countries; tightened security for our troops, our diplomats, our air travelers; strengthened sanctions on nations that support terrorists; given our law enforcement agencies new tools. We broke up terrorist rings before they could attack New York's Holland Tunnel, the United Nations, and our airlines. We have captured and brought to justice many of the offenders.

But we must do more. Last week, I announced America's first comprehensive strategy to control international crime and bring criminals, terrorists and money launderers to justice. Today, I come before you to announce three new initiatives -- the first broadly directed at combatting terrorism; the other two addressing two potential threats from terrorists and hostile nations, attacks on our computer networks and other critical systems upon which our society depends, and attacks using biological weapons. On all of these efforts, we will need the help of the Navy and the Marines. Your service will be critical in combatting these new challenges.

To make these three initiatives work we must have the concerted efforts of a whole range of federal agencies -- from the Armed Forces to law enforcement to intelligence to public health. I am appointing a National Coordinator for Security, Infrastructure Protection, and Counterterrorism, to bring the full force of all our resources to bear swiftly and effectively.

First, we will use our new integrated approach to intensify the fight against all forms of terrorism -- to capture terrorists, no matter where they hide; to work with other nations to eliminate terrorist sanctuaries overseas; to respond rapidly and effectively to protect Americans from terrorism at home and abroad.

Second, we will launch a comprehensive plan to detect, deter, and defend against attacks on our critical infrastructures -- our power systems, water supplies, police, fire, and medical services, air traffic control, financial services, telephone systems, and computer networks.

Just 15 years ago, these infrastructures -- some within government, some in the private sector -- were separate and distinct.

Now, they are linked together over vast computer-electronic networks, greatly increasing our productivity, but also making us much more vulnerable to disruption. Three days ago, we saw the enormous impact of a single failed electronic link when a satellite malfunction disabled pagers, ATMs, credit card systems, and TV and radio networks all around the world. Beyond such accidents, intentional attacks against our critical systems already are underway. Hackers break into government and business computers. They can raid banks, run up credit card charges, extort money by threats to unleash computer viruses.

If we fail to take strong action, then terrorists, criminals and hostile regimes could invade and paralyze these vital systems, disrupting commerce, threatening health, weakening our capacity to function in a crisis. In response to these concerns, I established a commission chaired by Retired General Tom Marsh, to assess the vulnerability of our critical infrastructures. They returned with a pointed conclusion: our vulnerability, particularly to cyberattacks, is real and growing. And they made important recommendations that we will now implement to put us ahead of the danger curve.

Former Commission Chair
Tom Marsh At the Ceremony

We have the best trained, best equipped best prepared Armed Forces in history. But, as ever, we must be ready to fight the next war, not the last one. And our military, as strong as it is, cannot meet these challenges alone. Because so many key components of our society are operated by the private sector, we must create a genuine public-private partnership to protect America in the 21st century. Together, we can find and reduce the vulnerabilities to attack in all critical sectors, develop warning systems including a national center to alert us to attacks, increase our cooperation with friendly nations, and create the means to minimize damage and rapidly recover in the event attacks occur. We can -- and we must -- make these critical systems more secure, so that we can be more secure.

Third, we will undertake a concerted effort to prevent the spread and use of biological weapons, and to protect our people in the event these terrible weapons are ever unleashed by a rogue state, a terrorist group or an international criminal organization. Conventional military force will continue to be crucial to curbing weapons of mass destruction. In the confrontation against Iraq, deployment of our Navy and Marine forces has played a key role in helping to convince Saddam Hussein to accept United Nations inspections of his weapons facilities..

But we must pursue the fight against biological weapons on many fronts. We must strengthen the international Biological Weapons Convention with a strong system of inspections to detect and

prevent cheating. This is a major priority. It was part of my State of the Union address earlier this year, and we are working with other nations and our industries to make it happen.

Because our troops serve on the front line of freedom, we must take special care to protect them. So we have been working on vaccinating them against biological threats, and now we will inoculate all our Armed Forces, active duty and reserves, against deadly anthrax bacteria.

Finally, we must do more to protect our civilian population from biological weapons. The Defense Department has been teaching state and local officials to respond if the weapons are brandished or used. Today it is announcing plans to train National Guard and reserve elements in every region to address this challenge.

But, again, we must do more to protect our people. We must be able to recognize a biological attack quickly in order to stop its spread.

We will work to upgrade our public health systems for detection and warning, to aid our preparedness against terrorism, and to help us cope with infectious diseases that arise in nature. We will train and equip local authorities throughout the nation to deal with an emergency involving weapons of mass destruction, creating stockpiles of medicines and vaccines to protect our civilian population against the kind of biological agents our adversaries are most likely to obtain or develop. And we will pursue research and development to create the next generation of vaccines, medicines and diagnostic tools. The Human Genome Project will be very, very important in this regard. And again, it will aid us also in fighting infectious diseases.

We must not cede the cutting edge of biotechnology to those who would do us harm. Working with the Congress, America must maintain its leadership in research and development. It is critical to our national security.

In our efforts to battle terrorism and cyberattacks and biological weapons, all of us must be extremely aggressive. But we must also be careful to uphold privacy rights and other constitutional protections. We do not ever undermine freedom in the name of freedom.

To the men and women of this class of 1998, over four years you have become part of an institution -- the Navy -- that has repeatedly risen to the challenges of battle and of changing technology. In the Spanish-American War, 100 years ago, our Navy won the key confrontations at Manila Bay and off Cuba. In the years between the world wars, the Navy made tremendous innovations with respect to aircraft carriers and amphibious operations. In the decisive battle in the Pacific in World War II at Midway, our communications experts and code breakers obtained, and Admiral Nimitz seized on, crucial information about the enemy fleet that secured victory against overwhelming odds.

In the Cold War, nuclear propulsion revolutionized our carrier and submarine operations. And today, our Navy and Marine Corps are fundamental to our strategy of global engagement, aiding our friends and warning foes that they cannot undermine our efforts to build a just, peaceful, free future.

President Theodore Roosevelt put it succinctly a long time ago. "A good Navy," he said, "is the surest guaranty of peace."

We will have that good Navy, because of you. Your readiness, strength, your knowledge of science and technology, your ability to promptly find and use essential information, and above all, your strength of spirit and your core values -- honor, courage and commitment. I ask you to remember, though, that with these new challenges especially, we must all, as Americans, be united in purpose and spirit.

Our defense has always drawn on the best of our entire nation. The Armed Forces have defended our freedom, and in turn, freedom has allowed our people to thrive. Our security innovations have often

been sparked and supported over and over by the brilliance and drive of people in non-military sectors -- our businesses and universities, our scientists and technologists. Now, more than ever, we need the broad support and participation of our citizens as your partners in meeting the security challenges of the 21st century.

Members of the Class of 1998, you are just moments away from becoming ensigns and second lieutenants -- and I have not taken as much time as you did to climb the Monument. *(Laughter.)* I thank you for giving me a few moments of your attention to talk to you and our nation about the work you will be doing for them for the rest of your careers. You will be our guardians and champions of freedom.

Let me say just one thing in closing on a more personal note. We must protect our people from danger and keep America safe and free. But I hope you will never lose sight of why we are doing it. We are doing it so that all of your countrymen and women can live meaningful lives, according to their own lights. So work hard, but don't forget to pursue also what fulfills you as people -- the beauty of the natural world, literature, the arts, sports, volunteer service. Most of all, don't forget to take time for your personal lives, to show your love to your friends and, most of all, to your families -- the parents and grandparents who made the sacrifices to get you here; in the future, your wives, your husbands, and your children.

In a free society, the purpose of public service, in or out of uniform, is to provide all citizens with the freedom and opportunity to live their own dreams. So when you return from an exhausting deployment, or just a terrible day, never forget to cherish your loved ones, and always be grateful that you have been given the opportunity to serve, to protect for yourselves and for your loved ones and for your fellow Americans the precious things that make life worth living, and freedom worth defending.

I know your families are very proud of you today. Now go and make America proud. Good luck and God bless you. *(Applause.)*