CONFERENCE ON CRITICAL INFRASTRUCTURE PROTECTION

ADDRESS BY ATTORNEY GENERAL JANET RENO

Friday, February 27, 1998

Lawrence Livermore National Laboratory

7000 East Street, Building 123

Auditorium

Livermore, California

(12:00 noon)

MS. RENO: Thank you very much. It is a very special privilege for me to be here today.

This laboratory is such a great institution and it has such a distinguished history. I can see why, after a half-hour with Bruce, I was the student since I had forgotten most of my chemistry. And it has been one of the most extraordinarily helpful and constructive half-hours I have spent in the almost five years I have been Attorney General.

This is an issue that is critically important to me: How we protect the systems and the networks of this nation that make its businesses run; how we create a system that can provide for the protection of our nation's defenses; how you get to the hospital emergency room on time; how do we protect those whom we hold dear from a threat of chemical weapons in a subway.

Our energy production and distribution channels, our transportation networks and our telecommunication systems are more vulnerable than ever before as we come to rely on technology more than ever.

This generation faces extraordinary challenges as we face the problems associated with weapons of mass destruction. This technology brings us a new century and a new world of incredible opportunities and of daunting challenges which, as Adlai Stevenson would say, stagger the imagination and convert vanity to prayer.

The government, including the Department of Justice, is facing these challenges head on and taking steps to ensure the protection of our critical infrastructures, but we know full well we cannot do it alone. To ensure the protection of our critical networks and systems, we must work as partners, true partners, with the private sector, with the academic world, with great institutions such as this, in this vitally critical effort for this nation.

I am here today to discuss what the Department of Justice, including the FBI, is doing to face the challenges. And I am here to hear from some of you what steps we can take to build a stronger, better, two-way, respectful, trusting partnership with everybody who has been so significantly involved in this effort, some for far longer than we have.

I want a partnership truly based on trust. As Bruce has indicated, in 1995 the President asked me to chair a cabinet committee that would assess the vulnerability of our nation's infrastructures and make recommendations as to how to protect them. The process we started led to the creation of the President's Commission on Critical Infrastructure Protection.

I would like to pay very special tribute to Tom Marsh, who did an extraordinary job. He did not just sit in Washington and listen to people. He went out to communities. He went to so many different places and listened to people because he knew full well how important it was to build a true line of communication in this very sensitive and significant area. And so thank you, Tom, for just some great and wonderful public service. (Applause.)

MS. RENO: As you know, the Administration is presently engaged in determining how to implement this report, so this conference could not be more timely. But one thing is certain, and the commission made sure of that: it is vitally important to the success of any effort that, it be based on the idea that infrastructure protection requires that we work together as never before.

It demands a partnership among all federal agencies with responsibilities for different sectors of the economy or for certain special functions, like law enforcement, intelligence and defense. It also requires a partnership with private industry which owns and operates most of the infrastructures. It calls for a partnership with academia and labs like the one hosting us today.

You have the scientific knowledge to develop technical solutions. I have already been through some of the process that you have been involved in, some of the processes that are actually critical to solving and protecting some of the very critical infrastructures that we have

talked about today.

It also requires a partnership with state and local law enforcement. They are used to robbers with guns, but there are new criminals out there who do not have guns. They have computers, and they may have other weapons of mass destruction.

The use of weapons of mass destruction or cyber attacks on infrastructures that could lead to events like power outages or telecommunications breakdowns are not hypothetical. They are not speculative. They can happen. And it requires, in the end, a partnership with the American people who have the right to expect that all of us, whether we are an attorney general or a general, whether we are a scientist or a business person, that all of us are going to work together to protect this nation.

The Department of Justice and the FBI, as I have indicated, want to be strong, good partners. Let me face up to an issue. Some people get suspicious of law enforcement. They say, "I do not want to cooperate. I do not want people to recognize my vulnerability. I do not understand the criminal justice system."

We have a responsibility to work through the concerns that people may have so that they trust us. And I am here today and have been involved in trying to do outreach to those responsible for critical infrastructures to make sure that we hear from you as to how we can be a better, stronger partner in the process. And I have learned today, just from this lab, so much that can be done.

There are other concerns. For example, private business may be concerned about confidentiality. Business does not want to have proprietary information made public. The FBI, on the other hand, has a duty to provide an early warning to the community to prevent further attacks. We must work together to see how we can walk that narrow line and ensure that we do our duty in terms of preventing further attacks while at the same time maintaining the confidentiality of the person or institution or business involved.

The Department of Justice and the FBI have a duty to investigate and prosecute most attacks on the infrastructure, but there are constitutional and other legal limitations on what law enforcement can and cannot do. Fourth Amendment protections against unreasonable search and seizures is one of our citizens most sacred protections.

We must work with scientists as partners to develop technologies and processes that enable us to obtain evidence in strict adherence to the fundamental protections guaranteed our citizens by the Constitution. The private company that is the victim of a cyber attack must likewise understand law enforcement's responsibility to the Constitution.

Some dare to suggest that the Constitution, the most remarkable document that

humankind ever put to paper, cannot keep up with modern technology. I say we must not and we will not sacrifice any constitutional protection in order to adapt to new technology.

We must and we will work with you to ensure that we will master the technologies and together, that law enforcement working with the private sector, working with the scientist, will make sure that technology can be adapted to meet the constitutional protections that are so critically important. But to do this, it is going to require that we talk together, that we work together and that we understand the problem. It may be a problem that a scientist can solve, but we need the Fourth Amendment expert working with the scientist to understand.

The FBI works daily to prevent attacks on the infrastructure. And it is prepared to immediately investigate if the attack occurs. United States attorneys and other Justice Department attorneys are available with technical expertise on a 24-hour basis to respond.

And if the plan is carried out, a cyber attack, if it is carried out by agents of a foreign state or international terrorist group, we have the responsibility as well under our foreign counter-intelligence authorities.

In the early stages of a cyber attack on an infrastructure or a power grid, we often have no way of knowing who was behind it, what their motive was or where they attacked from.

It is impossible to determine whether the attack is part of a terrorist plot, a probe by a foreign intelligence service, or a part of a national level military assault by a hostile nation state; or is it simply the work of a disgruntled insider bent on revenge against a supervisor; or is it a young juvenile hacker out to test his skills against the latest firewalls.

At the outset then, it may be premature to mobilize the military or redirect national intelligence assets.

What we do know, however, is that regardless of the perpetrator, his intent or his whereabouts, the intrusion in most cases constitutes a federal crime. This means the Department of Justice and the FBI have the authority and responsibility to investigate it.

Whether the crime is physical or cyber, we need to ensure that as we investigate we are coordinating with other agencies as appropriate. If the attack appears to come from non-U.S. persons located abroad, we would want to call on the intelligence community to assist in gathering information about the perpetrator's intentions; or if the attack seems to be part of a hostile nation's war plan or involves an attack on the Defense Department's own critical infrastructures, DOD obviously has a critical role to play.

Our challenge, our extraordinary challenge, is to identify the attack we need to know: When is it a straight law enforcement investigation that the FBI and the Assistant United

States Attorney or Criminal Division lawyer control? When is it something that the National Security Council takes over? When is it something that clearly becomes international as opposed to domestic, and therefore the State Department controls?

What this means is that you do not have any ready answers, but you do have to develop a process--and we are in the process of doing that--to determine when we hand it off from one agency to the next, how we work together to make sure that we adhere to constitutional protections, how we adhere to Fourth Amendment issues, how we continue to adhere to the Constitution.

Now Bruce said you had been talking about that this morning. We have been talking about it constantly in Washington, and it is an extraordinary challenge. And civilian agencies also have important responsibilities and capabilities. Whether it is the Department of Energy in the event of an attack on a nuclear power plant or an electrical power grid, or the Department of Transportation in an attack on our air traffic control or rail systems, all these agencies have crucial roles in the event of a crisis. But the fact remains that law enforcement initially will have the lead responsibility for responding to an imminent or ongoing infrastructure incident.

One example of the partnerships that we need to foster can be found in a major New York hacker case. The FBI, Secret Service, NYNEX and Southwest Bell and a number of private companies and universities worked together to identify and prosecute successfully individuals who had hacked into a telecommunications network, a credit reporting company and other systems.

Meeting our responsibility to protect critical infrastructures, in my view, is one of the central challenges for law enforcement as we face the twenty-first century. As our reliance on the Internet, on automated systems and on other technological advances increases exponentially with every passing month so do our vulnerabilities to infrastructure attacks. Law enforcement must be prepared to confront this challenge and be prepared to do so in partnership with other federal agencies, with the private sector, with academia and with state and local agencies.

And thus today I am announcing the creation of the National Infrastructure Protection Center at the FBI. The NIPC's mission is to detect, to prevent and to respond to cyber and physical attacks on our nation's critical infrastructures and to oversee FBI computer crime investigations conducted in the field.

The center will build on the important foundation laid down by the FBI's Computer Investigations and Infrastructure Threat Assessment Center, which has been subsumed into the NIPC.

To ensure the strong partnerships that I consider vital, the NIPC will include

representatives from the Defense Department, the intelligence community and other government agencies. We also very much want to and hope that the private sector will be a participant in this center, very much like it participated in the President's commission.

This is the surest, best, quickest way to build understanding, to learn from each other, to understand the responsibilities, the duties, the processes and the authorities that each agency or institution possesses. But let me be frank again. I know sometimes of the distrust that exists between agencies.

I want to hear from all concerned, all who are dedicated and vitally involved in the protection of our infrastructure; I want to know what we can do to build bridges of trust and understanding and communication, what we can do to better explain the role of law enforcement so that people can understand, what we can do to sit down with scientists and say, "Here is our law enforcement. How do we solve it?" We can do so much through this center if we work together.

To augment our partnership, we want to establish direct electronic connectivity with private industry and the Computer Emergency Response Team, or CERTs, which is located across the country. This is a significant departure from the way law enforcement has traditionally operated. But the challenges of infrastructure protection require imaginative solutions. And I consider our liaison and outreach to the private sector to be absolutely indispensable to our success.

One of the issues the private sector will raise is, "Why should we work with you in developing technology? How do we know that you will maintain confidentiality. What can we do?"

And in the last half-hour I have learned that I might find some examples here at the lab in the partnerships that you have built with the private sector in terms of determining solutions. It is fascinating what we can do if we will only sit down and talk together and build trust, recognizing that we all have one common objective which is the protection of this nation that we hold dear.

The partnerships that we envision will allow the NIPC to fulfill its responsibility as the government's lead mechanism for responding to an infrastructure attack. But the NIPC cannot just react from one crisis to the next. To do our job we will have to be able to prevent crises before they happen, and that requires analysis of information from all relevant sources including law enforcement investigations, intelligence gathering and data provided by industry.

Through partnerships between federal agencies and private industry and with interagency and private sector representation in electronic connectivity to all of our partners, the NIPC will be able to achieve the broadest possible sharing of information and

comprehensive analysis of potential threats and vulnerabilities. And through its Watch and Warning Unit, the NIPC will be able to disseminate its analysis and warnings of any imminent threats to a broad audience in and out of government.

This will enable private industry and government agencies to take protective steps before an attack. But, at the same time, we can take steps together to protect the interests of all concerned and balance the responsibilities of everyone involved.

As we build our partnerships, we must ensure that whenever possible we share equipment, technology and know-how with each other and especially with state and local law enforcement who are on the front lines. Local police respond with guns now, but soon they will have to respond with cyber tools to detect an intrusion, to follow through, to find the person, to hold him accountable; and we must be there working with them.

This equipment will be expensive. And you scientists will create so much new equipment so fast that it will be vital that we all work together in every forum possible to make sure that we avoid costly duplication, that we develop research according to sound plans that look both to the defense and the law enforcement and the scientific interest, and that we do as much as we can working together, sharing.

We have established a track record in this area, but we have much to learn, too. One of the most important technological partnerships is the one we have established with the Department of Defense. In 1994 Defense and Justice created a Special Joint Steering Program group and staffed it with both Justice and Defense personnel.

We developed products such as the prototype see-through-the-wall radar; more affordable night vision devices, which have been instrumental in supporting and helping the Border Patrol; concealed weapons and contraband detection systems; and improved lightweight soft-body armor.

In addition to working with DOD, we have developed partnerships with the Department of Energy and with the National Aeronautics and Space Administration.

We point out those as if they are unusual. We should come to accept such partnerships as a way of doing business in everything that those of us involved in the protection of the infrastructure do.

But all of this only begins to touch on the range of things under development and the technologies needed by federal, state and local law enforcement. As technology becomes more essential to the mission of the U.S. criminal justice system, it has become more important that we better organize ourselves to fulfill these new requirements, because neither federal nor local law enforcement can afford to be isolated from scientific and technological

developments.

Accordingly, I have directed the creation of a special working group to streamline the Department's management of research and technology development.

Finally, as many of you can sympathize, the information revolution has happened so quickly that kids in junior high school are often more familiar with the new technologies than your local sheriff or the FBI agent. We need to build a law enforcement work force that is educated and equipped to deal with the new technologies and knowledgeable and imaginative enough to think ahead to the next generation of problems.

The NIPC will help us do this by working closely with other interagency groups that are developing training for federal, state and local law enforcement personnel on cyber investigations and weapons of mass destruction.

By creating the NIPC, the Department of Justice is taking an important step: We are creating new partnerships with the private sector and with other government agencies to combat threats to the critical infrastructure.

I also have asked Congress to provide us with $64 million in increased funding to support our expanded efforts to protect the nation's infrastructure in fiscal year 1999.

These additional resources will be critical to support the NIPC and will also allow the FBI to create six additional computer investigation and infrastructure threat assessment squads to be deployed in cities across the country. And it will allow us to hire additional prosecutors to target cyber criminals.

As I mentioned earlier, however, not every attack on a computer network or infrastructure that is used in the United States constitutes an attack on our national security and, in fact, most do not. An unauthorized cyber intrusion could very well be, as I indicated previously, from a little hacker or a disgruntled insider. We will pursue those investigations as part of our law enforcement authority. But, nonetheless, part of protecting our critical infrastructure means working closely with the national security community to fight cyber attacks.

Cyber attacks pose unique challenges. Because of the technological advancements, today's criminals can be more nimble and more elusive than ever before. If you can sit in a kitchen in St. Petersburg, Russia, and steal from a bank in New York, you understand the dimensions of the problem.

Cyber attacks create a special problem, because the evidence is fleeting. You may have gone through this computer 1,500 miles away to break through another computer 5,000 miles

away. Simply put, cyber criminals can cross borders faster than law enforcement agents can, as hackers need not respect national sovereignty, nor rely upon judicial process to get information from another country.

If we are to protect our infrastructure we must reach beyond our borders. Cyber threats ignore the borders. The attack can come from anywhere in the world. We must work with our allies around the world to build the same partnerships that we talk about here at home.

And to that end, a little over a year ago, I raised with my colleagues, the ministers of justice of the P8 countries, the eight predominant, largest industrial countries -- Canada, France, Germany, the United Kingdom, Italy, Japan, Russia and our government -- the issue of cyber crime and urged that we join together in developing a common response. Experts from all our countries and departments worked together in the interim. And last December the ministers came to Washington to meet in a day-long meeting that produced agreement as to the dimension of the problem and produced an action plan that I hope can bring real results in the year to come.

We must join forces around the world if we are to begin to deal with the cyber crime that may affect one person or the cyber threat to our infrastructure that may affect the entire nation.

To do this we must work very closely with our colleagues in the defense and intelligence communities both here and among our allies. And this presents the new partnership. While I am building partnerships with the Department of Defense, I am getting to know the minister of justice and the minister of defense in another country. Sometimes the problem seems so big, but it is so critical that we address it and understand that this great, wide world is now one that can be traveled in seconds.

Together we will determine whether emerging developments are a national security problem, a law enforcement problem, how to attack it, how to proceed. But until evidence is obtained that an incident is a national security matter, it is important that we not jump to conclusions, that we not conclude that we must use extraordinary measures that defy our Constitution.

If it has been determined that an incident is an attack on national security, then the Justice Department has three distinct roles.

First, we can conduct a criminal investigation that runs on a parallel track with the national security elements of the case. Indeed, criminal investigations often yield vital information and leads for the President's national security advisors.

Secondly, we can utilize the FBI's counter-intelligence authorities and techniques when

our national security is under cyber attack from a foreign power.

And, third, we will ensure that any national strategy for dealing with a cyber attack is drawn up, executed and assessed with strict fidelity to our Constitution and to our laws.

I think this is the most extraordinarily challenging time that law enforcement has ever faced. Boundaries in this world have shrunk. Technology has burgeoned beyond man's wildest imaginations. It is a time for us to come together and realize that if we work together, if we talk together, if we trust each other and understand that we have one common goal which is the defense of this nation, we can make all the difference. If each discipline goes its own way, ignoring the other, we will not solve the problem, and this nation will be at peril.

This has been, in this one visit and about a brief half-hour, extraordinarily enlightening to me. And I go back to Washington confirmed in the belief that, based on the example of what you do here, we can make a difference and we can translate what you do here to so many other arenas and forums around this country where law enforcement, the private sector, the scientists are going to work together.

Thank you so very much for setting an example.

(Applause.)

(Whereupon, the address by U.S. Attorney General Janet Reno concluded at 12:35 p. m.)

--o0o--

STATE OF CALIFORNIA) County of San Joaquin) ss.

I, Susan Palmer, a Certified Electronic Reporter and Transcriber by the American Association of Electronic Reporters and Transcribers hereby certify that I reported, using the electronic reporting method, the proceedings had of this matter previously captioned herein; that I thereafter transcribed my audio recording to transcription by way of word processing; and that the foregoing transcript, pages 1 to 26, both inclusive, constitutes a full, true and accurate record of all proceedings had upon the said matter, and of the whole thereof. Witness my hand as a Certified Electronic Reporter and Transcriber this 28th day of February 1998.

Susan Palmer, CERT 00124 Palmer Reporting Services