PRESENTATION OF ATTORNEY GENERAL RENO

BEFORE THE ARMED FORCES COMMUNICATIONS

AND ELECTRONICS ASSOCIATION

Wednesday, February 12, 1997

Ritz-Carleton Hotel

Main Ballroom

McLean, Virginia

(8:07 a.m.)

ATTORNEY GENERAL RENO: Thank you very much. It is a real privilege for me to be with you, because I think we face together an extraordinary opportunity that staggers the imagination. We have an opportunity in the business of the Department of Justice and in law enforcement across this land to begin to link information that will be incredibly useful in helping us to solve crimes and, more importantly, to prevent crimes.

We have an opportunity in the Department of Justice and throughout government that we are already exercising to make government far more effective and far more responsive to its citizens.

The information technology industry science has given us some incredible tools, but with those tools come some extraordinary challenges for the Department of Justice. We see with those new tools that some of them end up in the hands of criminals and terrorists. We face attack on our information infrastructure through terrorist attack that gives us extraordinary challenges that we must meet together.

We face the prospect that has actually occurred indeed of a hacker who can sit in a kitchen in St. Petersburg, Russia, and steal from a bank in Chicago. We have the eternal balancing of privacy interests versus the need to catch the bad guys and to protect our property and our person.

To do this, we must acquire our tools, but we must build prudently. We must ensure links and interoperability within the Department of Justice and between the Department and all Federal agencies, and indeed all state and local law enforcement. We must make sure that we do not duplicate with expensive systems that could serve one use. We must plan ahead to ensure that we use the taxpayer's dollar as wisely as possible.

And we must buy prudently. We must ensure that the taxpayers of this country get an appropriate return on their dollars. I do not want to be known as the Attorney General who was responsible for buying some widget that was not necessary or an overpriced system that was far too expensive. I want to work with the private sector, and, working together, I think we can build and buy prudently.

Faced with these challenges, we have the challenge of keeping current, and just in the four years I have been Attorney General I realize that as each day goes by something we purchased within the time I have been Attorney General has become obsolete. How we do that, by appropriate planning, by avoiding waste whenever possible, by building carefully so that we build for the future and ensure currency is surely one of the great challenges the Department of Justice faces. But, working together with the private sector, with others in government, I am convinced that we can do that.

But the ultimate challenge that we face is how do we do all this -- how do we use the tools at our command, how do we build and buy prudently, how do we get the bad guys -- while at the same time protecting our Constitution, our rights of privacy and all the principles that we hold dear in this democracy.

I believe that we can do this. I am told by the private sector we do not want government snooping around in our business, and we do not want to be snooping around in your business. We would like to avoid that. But it was the private sector that first came to me when I was a prosecutor in Miami and said, nobody in this community is looking at what would happen if there was a sabotage effort directed against the information infrastructure of this community. What are you doing about it?

And I looked at him, me being a lawyer, and said tell me what to do. I learned so

much from that individual, who happened to be a CPA who had gotten interested in the whole area, and I am convinced, through a partnership between the public and the private sector that is respective of the privacy interest of the private sector but understands the role of government, that we can work together, number one, to defend against attacks on the infrastructure, number two, to solve it and detect it when it occurs, and, number three -- and as importantly -- to hold the people responsible for it accountable and see that they are brought to justice.

If we ignore attacks on our infrastructure -- and we have had them at the Department of Justice -- and say we are too embarrassed to admit it and we do not want to get involved in prosecution because it will be embarrassing to us, it is going to happen again and again and again. And you are going to need all of us to work together, because oftentimes the person who makes that attack is going to be in some far-off country and the forces of the State Department and our diplomatic apparatus will be critical in bringing that person to justice.

We are all in this together, and working together, respective of each other's interests, I think we can solve the problem.

To do this will require some steps in the Department of Justice that we have under way. First, we must work with other agencies in government and with the private sector to develop a personnel structure that can attack into government service some of the best and brightest in the information technology field. Now, some people say to me, how do you put up with public service. Well, you get cussed at, you get fussed at, you have to testify before Congress an awful lot. But there is no calling that I know that is more fulfilling and rewarding than to serve the people and to make a difference in their lives.

And so we must design a structure that will enable those in the information technology field to feel that they can serve the citizens of this country and do so in a positive manner.

We must form partnerships with the private sector. I think, working together, we can do so much. We must avoid focusing power in a few in the private sector and do everything we can to encourage innovation, to encourage that new entrepreneur who is just getting started, who has an idea of how to do more with less at least cost to the taxpayers.

At the end of his term, Dwight Eisenhower made a speech as part of a farewell to the country after serving two distinguished terms as President of the United States and after a heroic career in the military, and warned of the inappropriate

influences of the industrial-military complex.

I think if we remember what President Eisenhower said and if we move forward into the next century, we can, 50 years from now, look back and thank what the private sector and the public sector did together as partners, the right way, to serve the American people, to protect the foundations of our government, and to protect democracy as we have known it for the course of this nation.

And that is the ultimate goal of the Justice Department, to preserve our democracy and the rule of law, to put people first, to give people the tools they need to make their life a better life, and to make sure that those tools do not control the people.

So what are we doing in the Department? Unfortunately, in spite of the huge advances recently made in information technology, not enough has been done to modernize the country's crimefighting tools and to allow information-sharing. We would have a series of convenience store robberies at home, and I used to press the police.

Couldn't you develop some information systems that cataloged all the details with respect to one convenience store robbery and start making links, and then you would find that the green Oldsmobile with the battered right fender was a common denominator of five robberies, and that would lead you to some other matters and other clues, and you could solve these crimes much faster.

We haven't done enough of that. For example, although many Justice organizations have begun to modernize their operations by purchasing the latest hardware and software applications, not enough thought has been given to how these systems can be interconnected to enable the sharing of information not just within one community but across the nation.

As members of our justice community move forward to deploy the latest information technologies and integrate them into their existing infrastructure, these systems must be able to communicate with each other.

To date, only a few law enforcement agencies have begun to explore the concept of an interconnected multi-media criminal record that integrates all the information, pertinent information. It could be photographs. It could be fingerprints It could be DNA samples, outstanding warrants and arrest records. There is so much that could be collected appropriately and properly consistent with privacy right that could make a difference.

Within five years, we are going to see the capacity of law enforcement to respond to a crime scene, make a DNA test at the crime scene, match it with DNA data banks, make a fingerprint comparison at the crime scene, match it with fingerprint data banks across this nation, produce instant clues for police officers, shut dead ends right at the beginning, and make an extraordinary difference for the police office who is on the front line in America.

But we have got to make sure that as we develop the technology of DNA and better fingerprint technology that we link this incredible information with the technology that is now developing, has developed, and indeed must be linked.

But to do our business properly we need to address in the frankest, most open way possible, in positive, thoughtful discussion, the issue of encryption. This issue may be one of the largest issues that we face in law enforcement, the increasing availability and use of data-encrypted products. On the one hand, encryption is extremely beneficial when used legitimately to protect commercially-sensitive information and communications.

I think it is absolutely essential as we move forward in the information technology age to ensure appropriate, proper, strong encryption to protect commercial interests, to protect privacy rights. On the other hand, the potential use of encryption products by a vast array of criminals to conceal their criminal communications and information from law enforcement poses an extremely serious threat to public safety.

We've already begun to encounter the harmful effects of some limited encryption in recent investigations. In the Aldrich Ames spy case, Ames was instructed by his Soviet handlers to encrypt computer file information to be passed to them. Ramsey Yousef, who is one of the alleged masterminds of the World Trade Center bombing, and his alleged co-conspirators apparently stored information about their terrorist plot in an encrypted computer file in Manila.

In a child pornography case, one of the subjects used encryption in transmitting obscene and pornographic images of children over the Internet. In a major international drug trafficking case, the subject of a court-ordered wiretap used a telephonic encryption device, significantly frustrating the surveillance.

Some of the anti-government military groups are now promoting the use of encryption as a means of thwarting law enforcement investigations. In several major hacker cases, the subjects have used encryption to encrypt computer files, thereby concealing evidence of serious crimes.

These are just a few examples of recent cases involving encryption. As encryption proliferates and becomes stronger and becomes an ordinary component of mass market items, and as the strength increases to the point of denying law enforcement access to intercepted communications or physical evidence, the threat to public safety and commerce will increase exponentially.

However, let me make it clear that we don't want to expand our authority to surveil. We want to keep up with modern technology. I would just like to explain what law enforcement can do now. If I want to intercept a telephone call of a drug trafficker, I have to have probable cause to believe that he is using that telephone, that he is using that telephone for criminal conversation, and that I can gain evidence of a crime being committed, to wit narcotics trafficking.

I have to prepare a lengthy and detailed affidavit from the investigating officer. I have to approve it as the prosecutor, or people in the Justice Department have to approve it, and it has to be submitted to a court to get a court order authorizing the telephone company to tap that wire.

If I want to go do a search of a computer that is not encrypted, I go to the court with a probable cause affidavit to show I have probable cause to believe that that computer possesses evidence of a crime, and I can get a search warrant. But those orders are going to be worth nothing more than the paper they're written on in the future if the bad guys can encrypt the computer so that we can't break it and if they encrypt their conversations so we can't intercept it.

What does that mean to you? That means that crimes against the private sector, crimes against banks, narcotics traffickers are going to have tools that we don't have to commit crime, and we won't have the tools to prevent it.

Let's just put it again in a balancing of interest. Everyone must recognize the need for strong, vigorous encryption to protect commercial interests. At the same time, those commercial interests still need the tools of law enforcement to keep up with what is happening in technology today.

I would like to continue this dialogue with all concerned, because until we solve this problem we will not be prepared for the information technology age, and I am convinced in conversations with so many people that we can, indeed we must, work together to solve the problem.

There are many examples, though, of what we are already trying to do to use the information technology to help do our jobs better. When new FBI agents graduate from basic agent school at Quantico, they are issued a firearm, issued a

badge, and now they're issued a laptop computer, and it is an extraordinary experience to walk into an FBI office, even in some of the remote parts of the country, and find young agents, computer literate and ready to go.

Second, information technology has played a significant role in the FBI's investigation of the Trade Center bombing, the UNOBOMB, and the Oklahoma City bombing terrorist incidents. That technology enabled the FBI to collect, process, manage, and ultimately disseminate huge amounts of disparate data, and then apply new computer-based analytical tools to produce the intelligence required to successfully complete the investigation.

The Drug Enforcement Administration has recently designed and implemented a highly-upgraded communications network backbone which will allow its investigative and intelligence personnel to access and share in a secure manner a vast array of case data and imagery, including fingerprints, photographs, and video. Additional, DEA is developing a system that will enhance their mission for drug source determination.

As another example, DEA and the FBI created together Drug-X, a data base system that enables both agencies to share information on and coordinate activities relating to drug investigations. Drug-X is the first law enforcement system to utilize TRUSTED GUARD technology, which allows the FBI's classified network and DEA's sensitive but unclassified network to share access to the common data base while maintaining the proper security controls.

Another example is the Immigration and Naturalization Service's secure electronic network for travelers' rapid inspection, or SENTRI. SENTRI was designed to apply information technology solutions to the unique problems we face on our southwest border This initiative brings together the expertise and resources of the INS, U.S. Customs Service, DEA, the FBI, and the United States Attorney for the Southern District of California, as well as the State of California and the Government of Mexico. Under SENTRI, state-of-the-art technology is used to speed travel of low-risk border crossers while inspectors concentrate their efforts on travelers posing greater risk.

The Department of Justice spends just over $1 billion annually on information technology. One of my strongest goals is to ensure that we spend that money wisely. We need to make sure that we use it wisely, that it enables us to do our job better and more efficiently for the American people.

I believe that that means we need to use it to collaborate and cooperate with all members of the national justice community, to have the proper access to

information, and to share that information with each other. One initiative that I'm most excited about is the effort to build a global criminal justice information network. In outlining the administration's information technology initiatives, the Vice President has asked the Department of Justice to take the leadership role in coordinated this effort with state, local, and other Federal agencies. In many ways, this is our foremost information technology initiative.

Without effective and secure communication across all levels of government, within the national justice community we can never fully realize the full benefits of information technology.

All the technology and technology policies in the world will fail to support law enforcement unless our nation's justice community members can converse with each other and access necessary information from each other in a most secure, efficient and cost-effective way.

This effort will be conducted as a partnership, with all members of the Federal, State, and local justice communities. We must work with the technology industry to ensure the identification and proper application of the latest capabilities. The challenge to implementing a global criminal justice information network is difficult, but I do not believe it is impossible.

Many separate initiatives are under way in many existing systems and will need to be included in plans for this network. What we will be doing is developing an overall plan, including standards for interconnecting these systems, to create the network. As part of this effort, the National Institute of Justice is initiating a survey of the current state of the practice. The purpose of this NIJ survey is to identify existing systems and linkages, as well as needs and barriers to interconnection.

Believe me, if you travel this country as much as I have, there is a proliferation of systems with different names, different goals, different objectives, different means of communicating, and it just boggles the mind. If we can get them all going in the same direction, it is going to be one of the great tools that law enforcement has.

Of course, we at the Department of Justice must make sure that our own house is in order. Currently, many of the Department's components have separate information systems. This approach does not lead to fulfilling our department-wide objective of improved information-sharing, increased security, or cost containment.

I am working to change these past practices to ensure that we move forward toward a more unified information technology program that supports future information technology investments and achieve their objectives. We are developing a department-wide architecture. Once developed, the architecture will become the Department's foundational blueprint for the establishment of an effective and integrated IT operating environment that supports authorized access to departmental systems, the secure exchange of information, and improved communications across components.

It is frustrating to become Attorney General to discover that the FBI can't really communicate with the DEA, which really can't communicate with the Marshal's Service, which never talks to Treasury through modern technology. If we can get these agencies going in the same direction, we will have a powerful force to prevent crime, to solve crime, and yet to protect the privacy of all of Americans.

Information is vital to the mission of the Department of Justice. Our agents, attorneys and other personnel must have secure, timely, and reliable access to information. They must also be able to share and exchange information across organizational lines while being assured that the Department's information is safeguarded from unauthorized access and use.

Events such as the attack on the Department's WEB server have highlighted the need for us to develop policies and standards to improve the security and reliability of our network server systems, and we are going to have to have the best minds in government and in the private sector in the years ahead working together to see how we can ensure the security and privacy. We will not be able to do it working separate and apart. We must work together as partners.

At my direction, the Department's chief information officer is leading the effort to develop a security program that will take us into the next century. The Department of Justice has taken steps towards the consolidation and standardization of our own telecommunications network. This activity will result in improved information sharing, increased security, and further cost containments. This project will also provide the central point of coordination for other national justice community networking initiatives that I will discuss in a moment.

Another initiative under way is the improvement of our office management network, known as JCON. This initiative enhances the ability of our lawyers and enforcement personnel to meet the Department's mission of providing better law enforcement and litigation services to the public.

When I came to the Department, an FBI agent wrote up a file and it was at the

FBI. He brought his case file to the U.S. Attorney's office, and sometimes it was written up and computerized, sometimes it wasn't. Much of that was presented in court. If we can develop a system that permits these agencies to communicate together and develop a seamless flow of information, we can make such an incredible difference in enforcement.

More important, however, is that JCON will result in a standard technology for one-third of the over 100,000 department employees.

Another example that is already under way, part of the scene, is the Joint Automated Booking System. We will continue to work towards deploying the system, which redesigns and automates the booking process by means of the electronic collection, storage and transmittal of photographic, fingerprint, and biographical information about arrestees. This system eliminates redundant booking procedures, improves interagency cooperation, and facilitates information-sharing among Department of Justice and other law enforcement agencies.

JABS will improve the safety of law enforcement officials and the public by providing real-time operational information on offenders. Nothing is more frustrating to a local prosecutor, to the victim of a crime than to see somebody arrested, taken to jail, not properly identified, brought to court, let out on a low bond, only to find later that he is a prime suspect in another crime across town, a terrible crime, or that he is wanted in another state.

If we work together to meld these information systems so that we get current information as quickly and as accurately as possible, we can make such an extraordinary difference.

The technology issues confronting us are staggering, but we can deal with them if we are sure to put people first and take steps to ensure that technology does not control us.

This has been an extraordinary opportunity in these four years to serve the American people, to develop partnerships with state and local law enforcement, to reach out to the private sector, and to work together with them in all that I do. I think it is absolutely critical that the Federal government be a partner with all of those who care about this country and want to work together to address the critical issues.

But there is no issue more critical than how we go into this next century, committed to protecting the privacy of all Americans while at the same time

giving law enforcement the tools to do the job of preventing crime in the first place, solving it, and then bringing those people responsible for it to justice.

I have had the opportunity to work with so many in the private sector who have been thoughtful, careful, and wise in their advice. I look forward to continuing to work with you. I welcome your thoughts. And for all of those in government I reach out to you with the offer to work together in every way we can to meet these extraordinary challenges and to build a better America.

(Applause.)

(Whereupon, at 8:36 a.m., the speech concluded.)