Reboot Communications
Public Safety Technology Conference April 29–30, 2002
Web site: www.rebootnorthamerica.com

JANET RENO PRESENTATION

Thank you very much. It is a great privilege to be in this wonderful country. The ride up from Vancouver makes you think that you've been like a bird let out of a cage into one of the most beautiful worlds imaginable and I think, once again, that Canada is magnificent as always.

I have been asked to talk about public safety, focus on how technology and integrated justice initiatives can counter terrorism, and how law enforcement and the information technology industry can increase collaboration to improve public safety.

Terrorists use different tools. Sometimes it's a Ryder truck, sometimes it's a 737, sometimes it's chemical biological, or God forbid, nuclear weapons. It is extraordinarily important not to let the last event be the sole attention of our focus because next time it can well be something that we haven't even considered.

In determining these issues and focusing, and focusing as soon as possible on the correct alternative, science is often critical and we have seen on so many occasions what science can do, science and technology. But, what has not been addressed too often

in these last several years is the potential for cyber terrorism. It's probably harder to blow up a dam with explosives than it is to render the dam inoperable through cyber terrorism. In this instance it has been fascinating for me to see the challenges that exist with respect to cyber terrorism, but the opportunities, the benefits, the wonderful features of cyber technology and what it means to this world in terms of business opportunities, commerce, education, communication, long distance learning, inventory control that makes our companies so much more efficient, and yet, it also provides extraordinary new tools for law enforcement. Tools that permit us to link and order and prioritize information that becomes critical in the solution of a case, or in planning a crime initiative within a community. It is so important to think of what can be done, for example, with cyber technology in identifying, through public health methods, patterns that will lead us to understand immediately what the weapon is, or whether it's a natural epidemic, and what should be done to deploy.

However, the way I describe the challenges of cyber technology, the perils of cyber technology, is

that they are so significant that they stagger the imagination and convert vanity to prayer. When you think of the interconnectivity of the cyber world, the cascading affect of one breach that can lead to another industry, the threat to privacy and security, if we do not make provision for security. The threat of the evil doer, the terrorist, the Foreign Intelligence Service. Who has access to our cyber network? We don't know because we don't know who contracts with who. What hostile power might be afoot? Think of what can be done through cyber technology used the wrong way. Stolen identities, stalking, theft, and threats to an infrastructure, a critical infrastructure, power, transportation, the emergency response, water, sewer, bank and finance, food delivery. We have been very, very lucky ladies and gentlemen. When 90% of large corporations and government agencies report that they detected a breach in the seventh annual survey of the Computer Security Institute, we know that we're lucky that it hasn't gone further. Lucky because we have come into this cyber world and this era of cyber technology without preparation, without laying down ethical standards by which people can determine what should and should not be done. I will always remember

sitting in an advisory committee meeting in Washington of high level IT specialists when one of them said, you've just given me an idea. He said I realize my thirteen year old daughter knows that she shouldn't read other people's mail, she shouldn't go fussing through her brother's room, but she doesn't know when she can -- what she can do on a chat room, what she can do with other people's email, and it seems to me we've got to start teaching her.

Cyber technology came to us without a legal framework on an international basis, without a process or procedure to deal with it and to deal with the threats that it could create. It just grew like topsy, with no law enforcement emphasis, with no expertise, and with suspicion of either side, as the industry looked at law enforcement and thought we were trying to infiltrate and impair privacy without recognizing that the only way we could protect privacy was to go after the hacker and take effective deterrent action. Thus, the question with respect to cyber terrorism is, how we build a public-private partnership that protects. That protects security and privacy of cyber information and communication, and how we use cyber technology to assist law enforcement in its challenges it faces in

these days.

Here are some principles that I would like to outline for you. First of all, in a very general setting, but it applies specifically to the issue of terrorism and public safety. I think it is imperative that lawyers in this world renew their process and review their process for seeking the truth. When science, in the form of DNA testing, has identified one hundred or so people who had been sentenced to death or life for homicide, and DNA has determined that they did not commit that crime, that indicates to me that our truth seeking processes leave something to be desired. What about all the cases in which DNA was not relevant? What about cases which have not been tested? What are the -- what is the magnitude of our truth seeking failures? But, what it does, is show to me something more important. Lawyers sometimes think they have a monopoly on the truth, but, in fact, it is the scientists, the finger print expert, the DNA expert, the people that develop these techniques and tools that contribute so much to truth seeking. It is the physiologists and the doctors and the psychologists who are learning about memory, learning that as you put memory into your brain, it’s coded in a certain way.

As you pull it out two years later, it comes out, and as it is returned it is encoded with new information, changing memory, if you will. How does that affect our truth seeking efforts on the stand, in a jury box, in a courtroom? I think it is incumbent upon all of us to renew our search for the truth in a new way. With doctors, psychologists, scientists, DNA specialists, lawyers, and psychologists who can understand how we bring these disciplines together to find out what's happening. And the reason I think this is so important is that technology cannot be the only -- it does not have the corner on the truth market. It is going to be incumbent upon people to get to the bottom of an issue. I sometimes think, what lead am I missing? What fact have I omitted in my thoughts? What else can I do to find the truth? And I dig a little bit harder. At two o'clock in the morning on some occasions, as Attorney General, I was digging trying to figure out what was the piece that was missing that would give me sufficient evidence to justify an application to a court for a *Foreign Intelligence Surveillance Act* warrant. If you dig and you dig and you can't find the evidence, then it can't be made up, but it is so important to remember that one of the best tools for

preventing terrorism, for punishing for terrorism, is that detective, that agent, that has the sixth sense, that knows one -- what lead to pursue, how to pursue it and how to put a case together. To be frank with you, I think there are people who have focused long in the national security arena in which they don't have to justify their efforts before a court, as a detective does when he has to prove a homicide case, who do not have to justify a case that often before a court ordering a wiretap, and don't know what it takes to really make an ironclad case that identifies the terrorist, takes the preventative step that is so important. Takes it quickly, takes it early, and takes it in sufficient time to prevent the problem in the first place. So, with all the discussion of technology, I ask you to remember that behind the technology still exists human beings and the technology, in the long run, is no better than the human beings that are administering it.

It is imperative, as we seek the truth, as well, that we understand in this day and time of international terrorism that language and translation and interpretation in real time efforts is absolutely critical to our ability to prevent terrorism. The

nuance of the language, the nuance of an interpretation can give you two entirely different meanings and we have got to be prepared through whatever means at our disposal on both sides of the border, to be able to respond to the multiplicity of languages and then of idioms that exist around the world, and be able to make sure we hear the right one. Anything that can be done in terms of technology that permits translation, at least in a raw effort, that will narrow the scope of the enquiry can be so extraordinarily important.

It is important, thirdly, to remember that we are not going -- no one group, whether it be law enforcement or the private sector, is going to do it alone. We've got to do it together. As a state attorney in Miami, Florida, for fifteen years, I always knew that about once every six months the feds would come to town. They'd have some investigation that they wanted information on. They took our information, but they never gave us any back. And I resolved, when I went to Washington, to try to do everything I could to create a two way street. A two-way street recognizing that people in local law enforcement knew more about the community, more about the information that was available there, than the feds who were in town for a

day or two. And the feds might well have information on national security that if it fit with the local information, could produce a tremendous case, one in which we could both prevent and arrest and prosecute.

I think it is imperative that we recognize that we have got to have a partnership of the public and private sector. I think the public sector should take care of the security and privacy with respect to government cyber networks. And I think the private sector should take care of security and privacy with respect to private networks. But they have got to work together because with the interconnectivity of cyber networks, law enforcement will not be able to do it on its own. It does not have the expertise to do it on its own on a consistent basis. It needs the help of the private sector and that partnership should be formed. Now, people say, and I've been asked this already tonight, how can you get people to work together? Ladies and gentlemen, there is more than enough to say grace over these days. There's more than enough to be done without worrying about turf and who gets the credit. And if people are worried about leaks, the good detective, the good agent, knows how to build a relationship with the people you trust so that

you get the job done. But it -- we should be motivated by the fact that there is information out there in databanks, in a file, in so many different places that if brought together, can be the solution and the prevention of a terrorist act, that it is incumbent upon us all to start working together.

I was disappointed as I saw comments made around the country after September the 11th commenting on the fact that it was still a one-way street with the feds. It is imperative that we develop at the provincial level, at the local level, at the state level in the States, a two-way street that can benefit us all. It is imperative that we get the head of our law enforcement agencies involved and the chief executive officers of our corporations. There were so many companies or banks or others that I went to where the president or the chairman of the board didn't understand cyber issues and the vice-president in charge of information management did, but trying to get the chairman of the board or the president interested was more difficult than you might have anticipated. Unless we have everybody involved understanding the need for a joint effort of law enforcement and the private sector, we will never get the job done.

Switching a moment from cyber technology to other issues with respect to technology and science in terms of terrorism, another area that requires a close working relationship is between law enforcement at all levels and first responders at the local level. Those first responders are sometimes going to be the detective. The detective that figures out, hey, I'm a fireman and I've got to go in there, but this is what kind of chemical I think it is -- this is what I think this biological weapon is. We've got to improve our efforts to work together in this effort, recognizing that we must link the emergency rooms, the hospitals, together with fire, rescue, and do it effectively if we are ever to prevent deaths that could be avoided if we knew how to work together. But, in that connection, I would offer you one suggestion. I don't know about Canada, I suspect that you're much further along than we are, but in too many states in the United States, the public health, or the health departments, are woefully under funded, woefully lacking in the expertise and the experience to pursue some of these issues with respect to biological weapons. Woefully ill-prepared to provide alerts for epidemics that may be of natural causes or may be the product of

biological weapons. And I think it is important that we give support to the public health discipline and profession that can be a profound assistance in these efforts. It is also important, of course, for the state and the diplomatic side to work with the intelligence side and the law enforcement side in international terrorism. There's got to be an understanding of the issues and I think it is time when we look at the issues before us, that those detectives and agents who work in this area have extensive course work and study in the politics, the religion, the background of the efforts that they are investigating, because, again, it provides an information that can help lead to the truth -- lead -- follow the leads that give us the opportunity to prevent terrorism whenever we can.

One of the concerns I have, however, is that as we ask the private sector to joint with us, I can't speak again for Canada, but I worry that state and local and even the federal officials involved in cyber terrorism efforts do not have the equipment that is sufficiently current, sufficiently monitored, and sufficiently shared to be of use to everyone. I think it is imperative that we develop a plan for sharing that will

help us understand that this equipment is expensive. That if we sat down and planned in the States with the FBI, and said let's divide the country into regions, we don't need this expensive piece of equipment in every state, we can use it in four regions, we can give each other tickets and you exhaust the ticket and then you have to apply for additional rationing tickets, if you will, but everybody has a fair shot at utilizing the expensive equipment that is necessary. If we don't do this, if we don't share, if we don't develop a means of ensuring that we have the latest equipment, we're going to be woefully behind the bad guys down the road.

With respect to weapons of mass destruction, we can do so much if we work with the laboratories that are doing such great work in this effort. If we bring law enforcement together with the private sector and the academic world, and the labs, to do applied and specific research on detection of biological weapons, what is this particular weapon, how should we treat it, how fast can we learn about it, how fast can we deploy, what can the departments of health do, how can we work together to identify and to hold people responsible for such efforts? But, funding is an issue, and today, as I left Miami, I picked up the paper and people were

squabbling about the fact that they had incurred great expenses after 911 and there was nobody paying for it, despite the fact that Congress had appropriated extensive amounts of money. How you get monies down to the local level from a federal government is often a big question, but I think it is going to be imperative for us all to devise means of funding, of sharing, of holding people accountable for the monies they receive, so that we do it the right way.

We have got to make sure that first responders have the equipment they need to be responsive. Have the training with that equipment that they need to do it right and have the exercise opportunities necessary to bring all the players to the table so that we understand the implications of the particular weapon involved. Know what can be done with what we have and suggest what needs to be done with what we haven't. It is fascinating to think of what we can do with technology again in mapping, for example, if there was a nuclear blast, mapping what the implication for every area in a radius of five hundred miles would be and what the timeframe would be. These are the things that need to be done. We need to identify in every jurisdiction the issues with respect to who can be

quarantined and under what circumstances, and where they will be and who will be responsible for the distribution of medicines and what happens when it runs out, and how you cope and who gets what and when and why and where. Ladies and gentlemen, everybody should have to, at some point or another, go through drills and table top exercises in the most realistic fashion possible on all of these issues in order to be prepared. And even then, you wake up afterwards still thinking of it and still thinking of new issues that need to be resolved.

One of the major problems though in creating a two way street between the public and private sector is that the private sector doesn't like to report breaches of its security. Now, I have seen this before. I have been called by bankers long ago before I ever thought of threats of cyber terrorism. Janet, you're not prosecuting my embezzlement cases. Well, you haven't been reporting your embezzlement cases up until now. Well, I know but we've just suffered so much of a loss that we're going to have to report this one and nobody wants to take it. Why haven't you reported them before? Well, I just didn't want to put up with the publicity and I didn't want to appear weak and I didn't

want to appear vulnerable and I didn't know who to go to and when I went to them it took forever and we'd have the case set and it'd be set again and again and again. Whether it's cyber terrorism or something else, we have got to do a better job in the law enforcement community of identifying who you go to on issues of cyber terrorism or cyber crime so that we begin to build the relationships and people begin to understand the process. So much has been done in terms of integrated initiatives that enable law enforcement and the prosecutor to present the case in court and make a trial presentation to the jury through automated trial support systems that are staggering in their effectiveness. More can be done in presenting case management opportunities for the courts so that we can avoid the case where the case is set again and again and again, only to be rescheduled at the inconvenience of a number of witnesses. We can do this if we apply the knowledge we have to date in terms of automation and automated processes.

Let me tell you why I think it's so important that we do this. In the recent study that I referred to, 34% of the government agencies and the large corporations that reported, only 34% reported breaches

of their automated system to law enforcement authorities. Ninety percent reported breaches in this survey, but only 34% of those had been reported to law enforcement. But look at the cost, $377,000,000 last year, $455,000,000 this year, and only half of the people surveyed reported or quantified their loss. This is a critical time. It is a time when we must develop deterrents, when we must set standards for the use of the cyber technology that we have, where we must develop working relationships, and I suggest this to you, call the local bank, call the FBI, or call the R.C.M.P., talk with them. Figure out how you can work together to answer these questions.

I had a conference at Stanford University Law School and then in the east coast in Herndon, Virginia, which characterizes itself as the Silicon Valley of the east, and the question I put, before I left office as Attorney General, to corporate executives and security experts was, what can I do as Attorney General to address these issues and to give you confidence in law enforcement so that you can go to law enforcement and we can start forging precedent that sets the standards for the use of cyber technology. It was the leaks, it was I don't know who to go to, it was it takes too

long, it's too much trouble, it's a bother. Let's try to work through those issues and be responsive.

It is imperative, too, if we are to make law enforcement and the private sector comfortable with each other, that we have statutes that are common so far as possible around the world, in terms of what can be charged, what should be charged, what can be extradited, and the issues surrounding accountability. It is imperative that we have an international framework that permits us to trace on a twenty-four hour, seven day a week basis.

But, leaving that aside, I turn to the issue of communication. I was -- came to Littleton, Colorado, about two days after the tragedy there at the school shooting. All people could talk about was the terrible sense of frustration they had in terms of emergency preparation, in terms of communication with the emergency room, with families, with police, fire, first responders. The communication system simply broke down. We have got to make sure that in both countries, along our borders, that we have the capacity to communicate with all involved, and across our borders with each other if we are to make a difference.

People have asked me again and again, particularly

in these last months, do we have to sacrifice our freedoms in order to protect against terrorism? I say no. I had the privilege of presenting letters of apology to Japanese-American citizens. Letters of apology signed by the President of the United States and authorized by Congress. Letters of apology given to them because they were interned in internment camps in World War II, while in some instances their sons were being drafted to fight for this country. We recognized our mistake in my lifetime and I hope we do not make another mistake of lasting duration as we try, and I think we will be successful, in bringing the terrorists to justice. It is so important that we continue to strive in every way we can to adhere to the laws of our respective countries. To the guidance that has been handed down from one generation to another. In our instance, John Marshall said the *Constitution* was a living document and I think that this document can live through cyber technology, through the issues with respect to what can be done with it and without it. And I think we can be successful.

But, there is one issue that I am concerned about and I think we have got to prepare for it. What happens if there is an event of cyber technology? What

happens if there is a cascading affect on our interconnected network of cyber technology in the critical infrastructures of water and sewer, emergency response, transportation, food delivery? What will happen if there are no phones and there is no electricity? And what will happen if we see that those attacks are coming from a renegade country? We cannot identify who it is and they will not cooperate. What do we do? How do we do it? What is the law? How can we work together in addressing these issues?

I come before you with some pessimism because in 1998, Sam Nunn, after he left the United States Senate, spent a lot of time and effort trying to get this nation to be prepared in terms of information security and law enforcement and private sector cooperation. I had the opportunity to appear at a conference at Georgia Tech a year or so after Sam Nunn appeared and we had not done too much more in terms of cooperation between the public and the private sector. Now, the latest report indicates that the reporting of breaches of cyber networks is down reversing a trend that had been started upward. Sam Nunn closed his statement in Atlanta in 1988 -- 1998 as follows:

"My bottom line is, that as a nation, we have an

opportunity to act now in advance of a crisis. We must seize the opportunity rather than wait for either a perfect solution or an information security disaster to occur. We must not wait for a cyber space Pearl Harbor to strike us before we begin to take steps to protect our economic life blood."

I think that speaks volumes for where we're at in the issue of cyber technology and cyber terrorism and it is imperative that we act now. It is imperative that we act now to prepare ourselves and our first responders to be able to do everything we can to prevent terrorism. Through surveillance, through appropriate court ordered surveillance, but it is also imperative that have in place public health mechanisms, other mechanisms, that will help prepare us to deal with a crisis that will stun us all unless we take steps now.

I'm particularly proud to be here with law enforcement today. My working relationship with the Canadian authorities during the time I was Attorney General was to me a very gratifying one and I deeply appreciate it. For those of you who were involved, my hat's off to you and my sincere gratitude to you and all your colleagues. But this is a time, it is not an

ordinary time, it is a time for action, a time for collaboration, a time for partnership, a time for using science, the law and the human spirit to solve these critical problems before a Pearl Harbour occurs again. Thank you very much.

MODERATOR: Ladies and gentlemen, Ms. Reno is going to take a few questions and so -- from delegates that are here present at the conference and we have a microphone here that, if you'll take the microphone and speak clearly into it, that would be very helpful.

QUESTION FROM THE AUDIENCE: Madam Attorney General. Good to see you again.

MS. RENO: How are you sir?

QUESTION FROM THE AUDIENCE: I'm fine. Thank you for your comments, but I'd like to ask you, 911 showed that in the New York area we had almost a total breakdown in the ability to communicate. The police radios, there was an overload on the cell phones and so forth and they had to go back to -- to portable radio systems in order to communicate. And the federal government, through FEMA and others, was able to, in about two or three days, provide backup communications, but what do you believe needs to be done to enhance this inoperability that you spoke of and also to make sure

that there's seamless communications available to all elements of the first responder community?

MS. RENO: I'm not the expert, but I think it is imperative that we take each section of the country and try to devise a means of ensuring communication. At first I think it's going to be patch work as we learn more about -- as we work through the narrow banding issues and other issues we will come to have better understanding, but we have got to have backups, we've got to have plans. And I think it is imperative for all of us to try to focus on how we can develop the backups now and provide a master plan for ensuring appropriate communication for emergency, police and fire efforts for the future. And I think that applies in areas other than terrorism and other than in law enforcement. I think it applies with respect to hurricanes and everything else.

QUESTION FROM THE AUDIENCE: Thank you Madam Attorney General. What was your most disappointing moment as Attorney General and on a more positive note, what was your most gratifying moment?

MS. RENO: The most disappointing moment was Waco. We had asked so many questions, we'd been through it, we knew that we could not tell exactly what would happen

because David Koresh had talked about Armageddon, even he were not in any way given an excuse. John Danforth, the special counsel we appointed to re-investigate Waco, wrote me after I left office saying you did exactly the right thing. You couldn't walk away from four agents killed and sixteen wounded trying to execute a lawful warrant. Neither could you stay there forever. Delays of two weeks or two months wouldn't have made any difference because Koresh set those fires and he was out to create his own Armageddon. I will never know what the right answer was because that went to his death with David Koresh and if I had not done anything, he might have done exactly the same thing two months later and I would have been as condemned for it otherwise. But I think the agents handled themselves extremely well and it was the most crushing thing that has happened to me just thinking about those children.

And on the -- the high -- you -- I don't know whether you hear it in Canada, but you hear it in the United States, where people say, those bureaucrats and they can say, those federal bureaucrats with even more vehemence. Well, I have a special mission to let the people in the United States and any other country know that wants to know, what remarkably wonderful,

dedicated, fine, brilliant, able men and women work with them and for them in the Department of Justice and other federal law enforcement agencies. And it's, I think, the great time for me has been to serve with so many wonderful people.

QUESTION FROM THE AUDIENCE: Madam Attorney General, it's my pleasure to tell you that we have from Compact Computer a great respect for all that you've done in the service of your country and have been a model, I think, of public service. And my question is, in speaking with the -- with a person from the FBI, a highly placed official, at a conference, he indicated that one of his big difficulties was to send a simple email to conduct his business within the FBI framework. And, of course, it was a light moment, it was an evening reception, but we continued the conversation as we are, in fact, some -- somewhat of an expert in that area. And he said that he had requested of the officials that there be some alternative and he was told that there was not, that nobody should send an email unless it was secure and yet there was no mechanism for sending it. So, he asked if his superiors could make available to him a secure carrier pigeon, but that was his indication, that a lot work

needed to be done in that direction. So, could you indicate what is being done, if anything?

MS. RENO: I can't tell you what's being done now. I can tell you what I did when I came into office and discovered that the FBI had not developed an automated system of email or computer storage, data storage, or data connectivity, whereas other agencies had moved ahead rather substantially. We went to Congress and were not as successful as we would like in getting the monies initially. Louis, and I don't know whether he touched on it, then brought in a retired executive from IBM who, by the time I was leaving, was beginning to bring some semblance of hope to the whole process and, I think, was developing a system that was going to be effective. But, that was one of the great surprises for me and that's the reason I think it is so important that we use the tools that we have available to get the information linked because it was missing things. It was missing this piece of information from an agent's file in the west coast, that linked with this agent's piece of information, could have made a tremendous difference. But I -- I hope it's on its way to resolution and my informal understanding is that it is.

QUESTION FROM THE AUDIENCE: Ms. Reno, first I wanted

to congratulate you on handling the situation of the Cuban boy in Florida. I thought you showed tremendous courage there in a difficult situation. I'm actually with immigration in Canada and I wanted to ask you a bit about what's going on with -- with INS. You know, there's -- as the former head of the Department of Justice, you had INS under your wing as well, and there's been some proposals to break up INS, divide it into pieces, and I wondered if you could share any of your thoughts with us on that for a moment? Thank you.

MS. RENO: My concern is when I took office, INS was probably the most neglected agency and it did not have the infrastructure even in terms of personnel, in terms of automation, in terms of management, in terms of radios for border patrol cars, in terms of bullet proof vests for border patrol agents. We worked hard to try to develop that, but Congress preferred to give the monies for border patrol agents without providing the infrastructure that was necessary for that agency to function as well as it could. No restructuring of INS will work unless there are funds that will make it work, and unless there is flexibility in developing a salary scale and an employment capacity that can attract and retain the best people. I just -- you can

fiddle with structure and it may help, but it's -- you have got to have the funding to go with it and it's got to have the flexibility for the person who manages INS to get the job done.

QUESTION FROM THE AUDIENCE: Ms. Reno, I'm from the Canadian Department of Justice. Recently in American media, including *Washington Post* and most recently *60 Minutes* on Sunday night, there have been suggestions that the United States is at risk of terrorist activity from Canada and the suggestion has been that Canada is not doing enough to deal with that problem. Can I ask you if during your term as Attorney General, you were ever in any doubt as to whether Canadian authorities, Canadian officials were seriously addressing those concerns?

MS. RENO: My experience, and I was asked a similar question by the press just before I came in here, was that I got excellent cooperation from the Canadian authorities. I think, again, recognizing our borders are long and rugged, they -- the Canadian authorities have somewhat the same challenges that we have, but from my experience they were conducting themselves in a very professional manner in trying to solve it as best they could and I have nothing but praise for the

cooperation I received from Canadian authorities.

Thank you all very much.