ADDRESS

Cybercrime Summit:

A Law Enforcement/Information

Technology Industry Dialogue on

Prevention, Detection, Investigation and

Cooperation

Wednesday, April 5, 2000

1:45 p.m. to 3:05 p.m.

Stanford University Law School

559 Nathan Abbott Way, Room 290

Stanford, California

P R O C E E D I N G S

(Afternoon session began at 1:45 p.m.:)

ATTORNEY GENERAL RENO: Thank you. This has been excellent. What I would like to do is just ask a couple of questions about the reports, and then outline what I have heard and some additional thoughts and get your reactions so that I make sure I come away from here with your thoughts.

It seems to me that with respect to incident reporting the law enforcement representatives here, all of us have got to

be reminded we must do a lot better job just in terms of victim relationships. I mean that is what it is all about, whether it is a bank robbery and how we handle the bank robbery information or this kind of information, we have got to do a better job of it.

What I would like to suggest is that we develop Harris, if you thought well of this a small working group of people who would really be interested to develop a protocol that can be useful, a template, as you suggest, to overcome some of these issues.

And with that in mind, if you would be thinking about any other issue that might be relevant, it would be extremely helpful to me.

Somebody said law enforcement never leaks information. I think law enforcement has got to do a far better job of that. And we need to look at how it dissuades people from coming to law enforcement and make clear what we can and cannot do in that regard.

I am very interested in the CPA issues and would like to follow up on that.

One of the most difficult issues, though, is how do we keep you advised. One of the most terrible things I have ever been through was a long homicide investigation in which the victim's family was distraught. One of their members had been blamed for it. And it was a very long and tedious investigation. Not to be able to tell parents who had lost a child just what was going on was very, very difficult.

Somehow or another law enforcement has got to be able to conduct the investigation in a professional, proper way while at the same time recognizing the human concerns involved. And I think this is true here. I think we need to figure out what we can properly say and not say so that we keep you advised. We have got to develop timeframes by which you might expect answers.

With respect to the second report, I like the way you

destroyed the myths. I particularly think the first myth, I cannot think of anybody really that gets hurt because you think the headlines one day is a going to have a lasting effect and people forget headlines pretty quickly. But I think we have got to make sure that more people understand that because, again, it is so important we exchange information.

I think one of the keys to this, and I just cannot stress how important it is, the myth that industry does not want to be involved, does not want to participate has clearly been demolished here by the presence of so many. But we have got to continue to break that down. And I think the meeting on the East Coast will be helpful and follow-up working group meetings will be extremely helpful.

But the one thing I would suggest to everybody involved, the single most important thing that we can do is to develop a track record, a track record of competent investigators who know what they are doing, working closely with industry, leading to a successful conviction, an appropriate sentence that people talk about. And then we can truly talk about some of these cases. We can go over them. We can explain what worked and what didn't work.

And I just urge everybody involved to pursue, not just for the sake of pursuing it, but if you have a case that needs to be pursued, let us do so and let us try to work together to make it a model for others.

The third myth I think is clearly again a myth. But I think it goes back to the point I am hearing again and again, which is law enforcement has got to make a better explanation of what it is doing, what its problems are, what its limitations are and what it can do. And, again, the actual case properly done is one of the best messages.

Finally, the fourth myth about law enforcement not caring about impact on business. I have seen some investigators, very few and far between, and some prosecutors not give much of a darn about what their investigation did to people, but that is over twenty years and I can think of

two instances. And I did not have anything to do with one; I just saw it from a distance.

Most people do care. They sometimes get caught up in the press of their work. But I think we have got to be reminded again, and I think law enforcement has got to understand what would you feel like if it were your parent, your husband, your wife, somebody you loved dearly caught up in this, how would you like to be treated. What would happen if your brother was the CEO of the company that had been severely hurt by a hacker. How would you like your brother to be treated in that situation.

I think you all have touched here on resources. Somebody told me the other day the Justice Department salaries were not much, but I should not worry about salaries. I should worry about the cyberarchitecture of the Justice Department and the resources available and the automation of the Department. Because, I was told, that if I did not worry about it nobody would want to work at the Justice Department within three or four years because we were so totally old-fashioned, antiquated and out of date and people could get far more interesting jobs with far better tools at most other companies in the world. That is leading us to try to do something about it. But what again it points out is the need for law enforcement to share its resources, its expertise, it's equipment.

I had occasion after the morning session to talk to some of the representatives from California. Just think of what we can do, the public and the private sector, if we share training opportunities, if we share equipment where it is appropriate, if we share expertise. We can truly make a difference.

I think this is going to require some new approaches in the public-private partnership. But the whole point of what we are talking about is that we have, as Mr. Watkins said, an anarchist phenomenon that is everywhere, that everyone has come together to construct, to build, to enhance. It is rather an unruly, chaotic instrument we are dealing with, but the more we can work together to harness it, not so as to limit it but to make it even more useful, the better off

we will be.

I think this is going to require that we think through the issue of how we form public-private partnerships, how we take advantage of somebody from industry to serve for a time as an intern, if you will, and vice-versa. And I would like to suggest that might be another topic for conversation.

The final report was on the vulnerability information. This is key. I have had to deal with the issue of weapons of mass destruction for seven years now, what chemical and biological weapons could do, what nuclear weapons can do, what happened in Oklahoma City. It is one of the awesome responsibilities of government service. But when I think of what one mad genius could do with this remarkable tool, that also staggers the imagination and converts vanity to prayer.

There is before law enforcement and before the issue of investigations and the like what we can do together to prevent it, to prevent terrible destruction caused by manipulation of services controlled by automation. And that is going to require the differentiation between national security issues and law enforcement issues. And when it rises to the level of national security so we take appropriate action in emergency situations, I think we have got to include that in all our discussions.

What I would like to do, Harris, in connection with the vulnerability process is take the notes from this last report and try to develop contact numbers and points of contact and places to go and protocol that can give everyone clear information as to what can be done. We could include the National Association of Attorneys General, the IACP, the National District Attorneys' Association, and develop a network so people know who's who and what can be done.

Finally, there are a lot of issues, a lot of legal issues that deserve a great deal of thought and there are a lot of technical issues. I am wondering how we can continue on

this dialogue, how we can answer Peter Watkins' questions down the road, how we can answer my questions and your questions about what happens when the French man being investigated by the French authorities has committed a crime in France, but it is not a crime in the United States, or what happens if you are in a country where electronic surveillance of any kind is not authorized, that they have concluded the search of a computer is not a physical search, that it is an electronic surveillance, if that be the case, and there is no authorization for surveillance. There are so many questions that we have got to ask, both within our federalist system of government as between the fifty states and between nations.

What happens on so many issues. You can help us define those issues. And it might well be that we develop a working group, because there is no other situation that I know of where the interconnectivity of this medium brings public and private sectors together and where we are going to have to use new methods, not new legal methods, but new factual methods of getting to the truth.

The next issue is how we deal with crime that knows no borders. How are we going to prosecute. How are we going to bring people to justice. How are we going to put on trials. Who is going to be the witness. How are we going to make them available. How are we going to qualify them. There are just a lot of issues that are going to have to be addressed so that not only are they addressed here but around the world.

And the bottom line is: This is an instrument that covers the world. Our law will not limit it. We are going to have to work with our colleagues. And this is going to require some international contacts. I think that might be an interesting subject for another working group.

But I would be very grateful for your suggestions as to how we can continue this dialogue, how we can continue to answer questions and how we can possibly have troubleshooters, if you will.

If law enforcement comes to me and says, "I just met this most stubborn, butt-headed security expert for the ABC Company, what do I do about it?"

And I talk to the security expert at the ABC Company and he says, "That guy doesn't know what he's talking about. If he would just sit down and talk to me, I could get it worked out."

I would like to try to do everything we can through appropriate remedies to provide for the exchange of information that will permit the best discussion possible.

I would be grateful for the thoughts of everyone here now on this and any other issue that has not been covered in the reports.

MR. MEDRANO: Just a comment. As it relates to the international aspects of this, I think there is on May 15 a G8 meeting on cybercrime that I was invited to. I wanted to make sure that at least something from here is connected with that, which is happening in Paris on May 15, 16 and 17. So, as a delegation from the United States Attorney people going on there, and we are talking about cybercrime on the international level, not just United States.

ATTORNEY GENERAL RENO: Great. We will follow up on that.

FACILITATOR MILLER: Once concern, General, I have about that meeting, and I have already discussed it with Michael Sussman in the Department, and there is probably nothing that can be done about it, is it is a very formalized meeting, and that may be in the nature of G8 and

ATTORNEY GENERAL RENO: You cannot do anything about it.

FACILITATOR MILLER: That is what he said.

ATTORNEY GENERAL RENO: You can do a little bit about it, because what I try to do when I get there, you go through these long prepared you have these prepared things. And you read from them and people go through I mean you feel like

you are back in the 1800s in diplomacy and that this is how Jefferson must have presented his credentials in Paris.

But you find quickly on the sides of these meetings in bilaterals that you get an awful lot done. And sometimes, just sometimes, you can cut through the froufrou to get to the real issues. So you are right to have a concern, but I think they are extremely useful.

FACILITATOR MILLER: One of the things we could look at, as I mentioned this morning, industry is going to sponsor this global summit in Washington on October 16th and 17th. Maybe there could be an industry-sponsored break-out session where we would invite law enforcement. And that may allow a little more dialogue, if we had representatives of various countries where they would not feel so much compelled to stick to the script, so to speak.

ATTORNEY GENERAL RENO: I think that would be an excellent idea, and we would like to work with you on that score.

The other thing is I think we have an opportunity here in the western hemisphere with the Organization of American States. There is an awful lot going on. Most countries are not nearly as developed and they are quite willing to listen to us and make suggestions, respectful suggestions. And we could get this hemisphere working together on this issue. Because most farsighted ministers of justice and law enforcement officials I have talked to in the hemisphere realize how important it is.

The other thing is I think and let me give you just a little bit more of a statement than I did this morning. When I took office in 1993 we made a big push to develop a good working relationship with the EU and our counterparts in the EU.

I was told on so many occasions, "Janet, don't worry. I know you feel like you're getting nowhere, but we haven't really given much attention to the justice, home affairs, public safety issues because that gets so into the sovereignty issue." And they said, "Just you wait."

Last fall, as I mentioned, in Finland at Tampere they finally reached some understanding and moved forward quite rapidly in terms of finally focusing on home affairs and justice issues. They have told us, well, we still have to get our act together a bit and it will be the summer probably before we have a foundation upon which to build. I hope to be able to visit with my colleagues and with Jack Straw in June or July on this issue. And I would hope we could develop some really solid foundations in the North Atlantic agenda and the accent on this area, because it is going to be so important. And it will be important that we develop some understandings before it becomes set in stone in the EU.

FACILITATOR MILLER: Mark, did you have one?

MR. KADRICH: Yes. Mark Kadrich with Connection.

The government has eyes virtually everywhere, all over the world. And what I would be interesting in knowing is if the government would be willing to supply G2 on potential threats. If we can prepare for them, we would be in a position to react a lot quicker.

Certain organizations throughout the world have threatened the government. The government knows about it. And they are going to attack our government through our businesses. If we can take steps to prevent those attacks at the ISP level, I think we would be better off.

ATTORNEY GENERAL RENO: I would like to explore that with you because there are obviously some limitations there. But on the whole issue of what you are really talking about is economic espionage. And I think that is an area Director Freeh has really focused on. We have got much to do in that area. And I think that might be something that can be discussed as to what the appropriate role of each is. And that might be a very specific issue we could address.

MR. GARCIA: John Garcia. I am from the Joint Task Force for Computer Network Defense.

Ma'am, could you give us your thoughts on how DOD and specifically the DCIOs play into the partnership that is being worked here between government and industry?

ATTORNEY GENERAL RENO: John Hamre, the outgoing Deputy Secretary of Defense, has been, I think, instrumental in bringing DOD, the Justice Department and the FBI much closer together in developing a working relationship that we can build on.

We have had an opportunity to discuss a wide range of issues. And I think the person who will take his place, Rudy De Leon, is going to follow in his footsteps in that thoughtful effort.

Meanwhile, I think an excellent working relationship has developed between the DCI and the FBI, and that has got to be built upon, because much of it is a personal relationship, and I think it has got to be institutionalized.

I think one of the things we have to do, both with respect to the issue of economic espionage and otherwise, is do a better job of proactively identifying risk areas that are we wait until it happens. With appropriate action, and by that I mean from a law enforcement perspective, I think we can do a lot more. I think both Director Tenet, Director Freeh and I recognize that and are moving to take action in that regard.

The whole area of DOD, the State Department, the Justice Department, when I came into office, a Justice Department representative would look in and say, "That State Department, this is clearly a law enforcement matter and they are trying to boss us around."

And I would go over to the State Department and Strobe Talbott would say, "Janet, we are the chief of mission. Tell him to get in their elbows." And my message to everybody is this is a whole new world in terms of crime. Borders are meaningless with not just cyberissues but high-speed mobility and people's I think CNN has contributed

greatly to it because people now see a world they never really could understand before.

It requires strong new partnerships, and I think they are all in the process of being forged.

MR. GRAHAM: I am Robert Graham from Network Ice.

Myself and others in the industry are spending a lot of time on preventive measures against stop hackers before the crime occurs. The focus of this meeting has often been on the response after the occurrence of a hack.

What kinds of efforts is the Justice Department pursuing for also doing preventive measures? For example, interacting with the hacker groups, setting up sort of stings that might pseudo systems to allow hackers to break into, and that sort of thing?

ATTORNEY GENERAL RENO: I assure you I didn't plant you there to ask that question.

(General laughter.)

ATTORNEY GENERAL RENO: But the reason I would suggest, though I left this to Harris' design, was that the message I have gotten so consistently from industry is, 'Look, we can do a better job of policing ourselves and preventing it and providing security and making sure our house door is locked and that our windows are not open, and the like. You handle it after the crime has been committed. We do not need your regulation.'

I think there is probably a middle ground where if we show what we can do together in areas that are truly law enforcement, then we can work together in terms of prevention and do so much in that regard. It comes back down to what we were talking about a moment ago in terms of proactive efforts.

I need your advice on how I can perform in this area, how the Justice Department and the federal government can do a

better job in this area without the industry feeling we are intrusive, that it is Big Brother watching you, that it is those concerns that are at foot.

So I am one of those people who thinks all crime from violence to anything else is far better prevented than investigated. And I would like to do everything I could to prevent it.

If you think we have reached some understandings down the road, maybe we should do a prevention working group, too.

MR. KLUEPFEL: A short question. On the plane ride out I read the book called The New Jackals, the capture of Ramzi Yousef and the pursuits of Osama bin Laden.

I think in the reading of that book, it really brings out the value of joint task forces and the level of cooperation and the piece in there about the World Trade Center architect who came in and pointed out that the bomb was clearly aimed at the structural columns really, from my background, says a lot of the kinds of things we need to be worried about and the level of cooperation.

The NIPC's release of the E911 Worm Alert working with the SANS Network and other industry organizations to get that information out, it was obvious to me that it probably came out of the evidence analysis of an existing case. I think that is a tribute to trying to work the problem early on. And I was the poker at the other side on the 6E issues of evidence protection.

Because I think you have got to strike the vein, and we have all got to work harder to recognize the vulnerabilities we may have right in front of our eyes and to limit the risk of the exploit. You characterized a brilliant, misguided disrupter of the network. I think the capabilities are out there. I think the vulnerabilities are out there. And I think we have really got to work closely together along all the lines that were collected in the three panels.

ATTORNEY GENERAL RENO: I think all these points are well taken, and I think it is important for us to you are probably going to think I am stupid to raise this, but this is the most graphic way I can describe it.

When I was a little girl I learned how to milk a cow because my father was having to go in to work early and I wanted him to be able to stay there as long as he could, so I milked the cow. And I was one of the few people my age that I discovered knew how to milk a cow, because everybody had become used to the electronic cow milkers and they just didn't know how to milk a cow.

We are going to become used to this wonderful tool, this remarkable phenomenon that has been created. And we are going to make ourselves very, very vulnerable unless we provide the security, the safety and the reliability of it that is so important for it to work. And we are going to forget how to communicate and how to solve problems without it. So I think the bottom line is let's work together to protect it.

FACILITATOR MILLER: What I was going to do after John is sort of take my to-do list that I have taken notes on and see if I have got the right to-do list here.

One of the dangers I found hanging around with Attorney General Reno is you always leave meetings with a to-do list, and make sure we have the right to-do list out of the three working groups. Some of them are short-term to-dos. Some of them are longer-term to-dos.

ATTORNEY GENERAL RENO: Maybe you and I could get together and just figure out how we

FACILITATOR MILLER: How we do it, certainly.

MR. HANDLER: My name is Brad Handler. I work at eBay.

Madame Attorney General, I had a question concerning follow-up on prevention and the key to prevention.

I think one of the things I have learned today and over the last several years working at eBay is that prevention will actually deter people who are down the path of committing a crime. One of the things and being able to demonstrate that there is a prevention mechanism.

One of the problems we face, those of us who deal with consumers every day online, is getting law enforcement to recognize the seriousness of the crime and then prosecute it. Internet fraud, auction fraud is probably the easiest thing in the world to prosecute from an online crime standpoint because we have got all the information.

Time after time we provide that information to law enforcement both local, state and also federal, and are told that it does not meet the guidelines of the dollar value at which Assistant U.S. Attorneys or U.S. Attorneys' Offices will take the cases.

Can you give us any guidance on how we can convince particular U.S. Attorneys' Offices to take those cases for the preventive measure of demonstrating to the bad actors out there that people will punish you if you commit these crimes?

ATTORNEY GENERAL RENO: I cannot tell you to go to Congress and tell them to give the U.S. Attorneys more money, and I am not talking about myself because I am going to be gone and I am going to be sitting on the outside looking in. So I feel comfortable in that.

But with the resources we have, if we can develop some common understandings about how law enforcement can participate with industry in sound, proper prevention programs, that is one of the best ways to proceed.

Secondly, in a totally noncyberrelated area of bankruptcy fraud, the trustees came to me and said, "People know just about where the radar screen is and they can get in under the radar and go right in with $25,000 here or $30,000 here and the U.S. Attorney says it is too small a matter to prosecute." We have since then started to confuse them as

to where the radar is. And I am told it has had a salutary effect.

We never have all the resources we would like to have to do everything we want to do for the American people. And I don't think there will ever be a prosecutor who has that luxury. But we try to work with the industry involved, with citizens to use our resources as wisely as possible. And that may be one of the ways.

The second way is to get state and local law enforcement trained in this, as well, and to make them a full partner in this effort, because the bottom line is that state and local law enforcement is on the front line in so many issues of law enforcement on so many crimes. And they can be a powerful partner. So there is much that can be done, and we would like to work with you in that regard.

FACILITATOR MILLER: Well, again let me try to pick up some to-dos. I am sure I missed some things, but let me see if I can pick up some things here.

One, several people have talked about the dialogues, so I think a to-do item is to decide whether we want to institutionalize meetings like this on some kind of a regular basis, number one.

And, number two, whether it should just be the IT industry and law enforcement, or whether it should be the broader set of industries involved in the Partnership for Critical Infrastructure, for example.

So I think we need to decide that, because if people decide after this meeting and the following meeting we have on the East Coast that this is a good idea, then there may be some value in regularizing it. Obviously topics can change from meeting to meeting. But clearly having a meeting on a regular basis becomes a forcing function in terms of making sure that both sides are continuing the dialogue getting working groups going. So I think that is a question rather than a to-do, but I think it is something we should decide in the fairly new future.

Secondly, picking up from both Group 1 and Group 2 and then the protocol you talked about, General Reno, about some kind of better way of dealing with victims and some of the things that Mike Vatis, in particular, reported on is developing a cook's guide for the business community on what law enforcement does in cybercrime investigations, for lack of a better term.

And then Bill was particularly commenting on what would be needed in the case of criminal investigation. I think that again would be a joint effort between the law enforcement community, perhaps with feedback from industry to make sure it is understandable and clear and not overly technical.

ATTORNEY GENERAL RENO: I think industry has got to be part and parcel of it, because as you all get into your technical stuff, and some of us do not understand it, we get into some legalese, into some jargon, and 6Es and things like that, and we need your onhand observations, I think.

FACILITATOR MILLER: Great. Well, we would certainly be willing and interested in partnering and developing a document like that. And then, of course, related to that is how to disseminate it.

And I think, again, Bill, in your group we thought that industry would be willing across-the- board to help disseminate it once it was developed, much as what was done with Y2K and other issues.

Thirdly was an issue that came up in several contexts, which I think again is more of government than industry, is elevating the issue internally within law enforcement. And then also, as John was suggesting, even taking it perhaps to the issue of educating judges about these issues.

Fourthly is working through this issue of confidentiality so that industry does better understand that, what really is being said by law enforcement. And I think again that is going to require dialogue back and forth. I don't think that is anything that is one side or the other.

ATTORNEY GENERAL RENO: Well, first of all, I think government is going to have to resolve itself. Have you ever been puzzled, you hear somebody say, "I'm sorry, the government neither confirms nor denies it has an ongoing investigation." Then you suddenly see a headline saying, "Federal government investigating so-and-so. Such-and-such says." There are a lot of guidelines. And we have got to you can help us address the larger issue.

FACILITATOR MILLER: Fantastic. We would be glad to do that.

In terms of a point that again the Group Number 2 made, report, was I think an interesting point, that the policy at the company, corporate level may be to cooperate with law enforcement, but that message may not have reached the front-line people in these companies. I think that is something industry needs to take a look at, how they do not send or have ambiguous messages internally in terms of cooperation with law enforcement. Again I think if we could develop this cook's tour to how law enforcement does these investigations, that might help to create more common policies within corporations.

Again, policies may vary from company to company, but at least there would be a template that people within a company could start off from and then they could modify to suit the particular company policy on sharing information.

The Ride Along Program I think is an interesting idea, Mike. And maybe we need to figure out what that would look like in the real world and how we would do a better job.

We have tried, as you know, General, at your suggestion, to set up a personnel exchange between industry and government. It has been a little hard to do that because I don't know that I think Mike is kind of strapped for funds these days, as everybody is, but I think we want to continue to work on that. I knew at least some of my member companies are interested in doing a personnel exchange, where they would send senior people for short-term assignments into the government. But we have to figure out how to implement that.

You mentioned the protocols on victim relationships. That is a joint effort between industry.

ATTORNEY GENERAL RENO: That would be in the guidebook.

FACILITATOR MILLER: And that would be part of the guidebook.

In terms of resource issues, it came up in a couple of the reports, and you brought it up again, General, in terms of sharing training opportunities, sharing equipment and obstacles that apparently exist now. I think industry needs to understand better what those obstacles are. As Howard Schmidt reported, many times industry wants to help and then it turns out that...

ATTORNEY GENERAL RENO: That there is a federal advisory committee regulation or you cannot do this or you cannot do that.

FACILITATOR MILLER: Right.

ATTORNEY GENERAL RENO: I think this is going to be the impetus for new approaches and new sharing.

FACILITATOR MILLER: In terms of the specific recommendation that Mary Riley reported on and the idea of industry figuring out a way to simplify ways for law enforcement people to figure out who within the company is the appropriate contact, we need to work that through. I think there is a desire to do that, but I think there was some disagreement among the companies about exactly the best way to do that. But certainly we want to make that as simple as possible.

I think what we all agreed on the industry side that does not make sense is try to have some master list that ITAA or the Chamber of Commerce would maintain. That is impossible. But how companies would do that most effectively without Intel or Microsoft putting a big black box on its front page of its website saying, "Come here if you have a crime to report," which is not exactly I think what the webpage

designers would be very excited about, but something that would really be able to work.

We mentioned the international, trying to figure out how to deal more directly with the international. Again, as I said, we are trying to do that on a global basis, but we would be willing to work with you in a way that would be most effective.

Then the point that Rob Graham brought up about the need to perhaps focus part of the next meeting on preventive issues as opposed to more investigative issues and perhaps using the meeting on the East Coast, devoting some time to that topic and continuing the dialogue in that area.

MR. SCHMIDT: Two quick things. One of them, since Hank brought up the issue in the 911 Alert that came out the other day, something that I don't know that we have discussed as a group, but the technical accuracies of some of those bulletins just created a tremendous nightmare of tech support. That came out. We were not aware of it. Since it affected some of our stuff, the next thing you know the support issue went up, everything went up, and there were some technical inaccuracies.

Not wanting to slow that process down, but to be able to sit there and be part of that process, and I would presume some of the other companies' representatives who have those products out there would be appreciative of the opportunity to comment and help define the technical accuracy of that and be prepared for the support level. Because when you start getting those calls at two o'clock in the morning and you are not aware of it, it is tough to give people the answers they need.

And the second thing, and this is something I believe is directly within your ability to do something with, is on the NCTP, the National Cybercrime Training Partnership, and the training for the state and local law enforcement folks, there have been a number of the companies in this room that have wanted to help support that training effort, but it has been difficult because of not wanting to involve

private-sector organizations in that sort of an emphasis and do the training thing.

So if you could help break that up we can probably provide more resources, the technical training that is necessary.

ATTORNEY GENERAL RENO: What I am going to have to do is to look at the public-private partnership efforts that are involved. This has been one of the most frustrating things I have dealt with, because at home I could form could call so-and-so at the local bank or somebody at one of the big eight firms and start talking about things immediately and did not have to worry about federal advisory committees, and the like. There are some significant limitations.

I think again in this area, considering the interconnectivity of the net and how we are all in this together, if you will, there are going to have to be, if current law does not permit it, there are going to have to be some relaxations that permit far better exchange than we have now. So I am committed to doing that.

FACILITATOR MILLER: With that I would like to turn it over to General Reno for the final comments.

ATTORNEY GENERAL RENO: I would add just one and that, again, gets into the issue of what can be done public versus private. I mean in a public-prevent partnership. The whole issue, Mr. Diffie, that you were talking about in terms of just the legal issues involved and legal issues that we might not have even thought of and why don't we start thinking about them.

And one of the things that industry taught me quickly was many of these legal issues can be solved by technical and technological advances so that you do not need legal adjustments. The more we can work together using, applying the technology and the law together the better we will be.

I can't thank you enough. I know how busy everybody is. And to spend this amount of time on this subject has been very important to all of us in the Department of Justice. And I

want to express my gratitude.

This is an extraordinary time. Never have we been there at the beginning of something where we can so shape it for the future into being such a remarkable tool for humankind. Your willingness to spend this time today is evidence of what I have found in this country.

People say we're cynical. They say we're selfish. They say we are isolated and we are very private. But there is tremendous goodwill in this country and certainly in this room today. Thank you very much.

(Applause.)

(Whereupon, the Summit concluded at 3:05 p.m.)