Internet Security Policy Forum II
"Understanding Risk and U.S. Economic Security"
March 22, 2001
U.S. Chamber of Commerce (USCC)

Closing remarks by Senator Robert Bennett:

I understand you had a good conference, and a lot of good presentations. I understand you heard from Doctor Rice. I met with her several weeks ago to talk to her about the issue of critical infrastructure protection and went through my standard litany, listing the problems and she was very polite and listened very properly. She then made it clear, in about three sentences, that she knew as much or more than I did about it and had been thinking about it for a long time and thinking very deeply.

One of the things that impressed me about our conversation was that Condoleeza Rice was not only a college professor who understands these things from an intellectual point of view, she served on a number of corporate boards and faced the problem directly in terms of corporate governments and corporate responsibility. I think it is delightful that we have a National Security Advisor who has that kind of background and that kind of insight. I understand that her presentation to you made that clear and helped you to understand that this is going to be a top priority for the Bush Administration. I was delighted to hear that from her, realizing that I was behind where she was in understanding the curve. Usually I'm the one who is helping people understand these things. It's a little humbling, considering we senators need to be humbled from time to time, to find somebody else who is ahead of us. So, I congratulate you for having had her, and I'm looking forward to reading her remarks myself as we go forward on this.

Reference has been made to Y2K and the more I deal with this, the more I realize the parallels that are here with respect to Y2K. Originally, I could summarize it in one sentence, which I think I shared with you last year. That Y2K helped me to understand what would happen to the economy if all the computers shut down by accident. Then I started thinking what would happen if they all shut down on purpose. But, I kind of thought that was the end of the connection between the two. As we get into it, we begin to realize that there is a great deal more that is parallel, if you will, between Y2K and this challenge. And I understand that Dr. Rice indicated that the initiative the administration is going to put forward, will be patterned, to a certain extent, to the Y2K initiative when there was great cooperation, rather than regulation between government and industry. I think that is a good pattern to follow. But, here is the other connection that has occurred to me as I continue to dig into this:

We realized fairly early with Y2K that the problem was not necessarily your computers, or the government's computers. And not necessarily one agency's ability to keep their computers running. The problem that threatens the economy comes at the connections; where your computers are connected to my computers, and if your

computers aren't right, they could transmit problems that my computers would then have to respond to. As we held our hearings on the Y2K committee, we focused increasingly on that issue of connections. It is just fine for power company A, and power company B, and power company C to be able to say their computers were all fixed for Y2K. But what about the overall national grid? And if there was a problem in one part of the grid, it could transmit itself in such a fashion that companies A, B and C could have difficulty communicating with each other and it could set off difficulties that would come down our grid to effect us.

The same thing, obviously, is true with respect to the critical infrastructure situation. The internet was designed to share information. It came out of a desire to get around quickly to a whole bunch of databases that are not yours, but that you want to get in to. The whole structure that we're dealing with, with the Internet, is an open structure designed to facilitate looking into everybody else's backyard. When you start thinking about issues of privacy, you don't want to automatically put privacy into a system that is designed to violate it. People don't think of the Internet in those terms, but that's really how we structurally put it together.

Now as we talk on Capital Hill about privacy and think about it a little more deeply, we begin to realize that the issue is not privacy. Do we want privacy on the Internet? What's the difference? Well, put it in the form of a transaction. If I walk into your store, and you have a gadget that I want to buy, we want to eliminate privacy for just a minute. I'm going to give you my credit card and you're going to want to know who I am. I'm going to want to know that you have these goods and you can deliver them at my house at 3:00 tomorrow afternoon, or whatever deal we make, if I'm not walking out of the store with them. And you're going to want to know that my credit card is up to date, and that I have enough money to pay for them. So, there's a violation of privacy on both sides. I know about your operations and you know who I am. And neither one of us is worried about that if we feel secure that you won't run out and tell everybody else what you found out about me, and I won't run out and tell everybody else what I found out about you. We have a transaction that invades privacy, but that doesn't upset either one of us, because it is secure. That's the challenge in the cyber world. We want the information to flow freely. We simply want it to flow between people who can guarantee that once they receive that information, they will keep it secure. So, it comes down to, "I'll show you my security protection, if you'll show me yours." And again, that was part of the solution to Y2K.

You may remember within the whole Y2K circumstance, we went to the Securities and Exchange Commission and they required companies to reveal, on their quarterly and annual reports, their level of Y2K preparedness. And initially, a lot of companies were not willing to do that. A lot of companies were very nervous about that. It was very interesting the reactions we got. "Well, if my share holders know how far behind the curve I am on Y2K, they'll sell my stock. So I don't want to reveal anything." "Well," say the lawyers, "if people know how much Y2K vulnerability there is in this company and something goes wrong, they will sue us. So let's tell them that everything is fine." I never quite understood the logic behind that, but that came out of a lot of the legal

departments. The other one, this also came out of legal departments of major banks, "do not promise anybody in writing that we will have the Y2K problem fixed. You can say, 'we're working on it,' you can say, 'it's a top priority in the bank,' you can say, 'the bank is confident that they will make significant progress on Y2K,' but don't ever, particularly in writing, tell a customer 'we will have the Y2K problem fixed.' Because if you do, and we have a problem with their account, they will then be able to sue us for all the money in the world. So, don't tell."

Well, as I said, we used the SEC to break through that. We said as part of your disclosure to your share holders, and therefore to your competitors and everybody else, "you must disclose your level of readiness with respect to Y2K." And it had the effect we wanted, it made a whole lot of public corporations far more interested in solving the Y2K problem than they were before. I see a clear parallel here.

You've heard a lot in your panels, and I was going to talk more about it, and I won't now because you've heard from the panels about the major source of threats to your security, and that's your own employees, disgruntled employees. I used to be in the retail business and the same thing was true there. You have a term in retail, we call it shrinkage. That's a fancy word for people taking things from you, and your inventory shrinks. Well, you'd like to think that most of the shrinkage comes from shoplifting, but in fact, in the retail world, most of the shrinkage occurs from either incompetent, or dishonest employees. Incompetent employees don't mark down the goods during sale time properly, or mark them back up when the sale is over, so they get sold for less than they should be sold for because the price tag is wrong. That's a form of shrinkage. Then the employee simply taking stuff home is another form of shrinkage.

The same applies in this new world in which we live. Incompetent employees can compromise your security. Dishonest or disgruntled employees seeking revenge can compromise your security.

Now, in the retail world you can always tell who the high shrinkage operator is. In our corporation, the word was, "a high-shrinkage manager is a high-shrinkage manager no matter where you put him." In other words, he runs a store in New York City and he says, "well, the shrinkage is due to the high shoplifting rate in New York City. If I ran a store in Madison, Wisconsin it wouldn't happen." Then you transfer him to Madison, Wisconsin and the level of shrinkage that occurs in the store there matches the level that you had in New York, it's just the way that manager is. He doesn't get his hands around that particular problem.

I think the same thing will apply here-that a company that is sloppy about their own internal procedures for security, again I stress security as opposed to privacy, is going to be sloppy all through the whole company. This is a CEO issue. It's a matter of company culture, and if the company management doesn't take it seriously, and says, "no, it doesn't really matter, it's not really a big threat. I'm not going to worry about it," not only does that company have the potential problem that will come from that kind of lackadaisical attitude, but you too have that problem if you are connected to them.

The Internet, again, was created for the purpose of sharing information and connecting everybody. When we get the benefit of that sharing and that connection, we also get the threat that comes from connecting with somebody who doesn't have the right kind of security.

Alright, what's the role of government? Dr. Rice made the comment, and I absolutely agree, that it should not be a regulatory scheme, it should be a cooperative scheme. However, again, going back to the SEC example with Y2K, I think it's appropriate for government to facilitate transparency on the question of "how secure are you?"

Now it may seem like an oxy-moron to be discussing transparency and security in the same sentence. But in fact, it's not because we come back to the same line, "I'll show you my security control, if you'll show me yours." If we have transparency and understanding at the level of preparedness, and expertise in networks, then we can get confidence between those networks, because I know it will be held secure and that the disgruntled employees of that company won't be able to hack into the disgruntled employees of my company because they have protocols in place that will trigger awareness of those kinds of attacks very quickly.

That is the final thought I will leave you. We should focus not on fire walls to keep everybody out, because if the main problem is disgruntled employees from within, or leaks from other people with whom we are connected, the firewalls that keep everybody out become kind of like the magical line that the enemy comes around quickly and suddenly it doesn't do you that much good.

I would recommend to you that you think in terms of controls that monitor aberrations, so that when something occurs within your network that isn't normal, you get a notice soon enough. Not after the fact, not "let's go back and try and reconstruct it," but "wait a minute, something has happened that is not normal." Now, it is very difficult to create a protocol that will track what is normal. But there are those who do it. I've visited some of the companies that are in the business of doing that and they're making pretty good stride. Once you get the protocol in place, and then the computer is running, as long as everybody is doing things that you have determined, not an outsider, not a government agency, you have determined this is the normal course of business, everything is fine. Then suddenly something happens that is not normal and you get an immediate red flag. You say, "well, what is this? Is this an incompetent employee who just pushed the wrong button in the wrong way? It's very easy to fix, teach him how to do it right. Is this a disgruntled employee, who is trying to break into a place where it isn't normal that these kind of intrusions should take place? And does it come from the outside? We've told all the people we deal with on a regular basis that this is how things work here and is this somebody from the outside who doesn't know how we do things? Who is looking for passwords or money or other database information that they shouldn't have? What is this?" And you can then start checking, with enough time, instead of after the damage is done.

Now, the people who are in the business that I've looked at say the vast majority of violations of protocols that they track with the programs they've created, are mistakes. They're not militias. They're just errors. Well, there's a business benefit from knowing that in and of itself. If you know it's your employees that aren't doing things right, and there are errors, then it's a good business procedure to be able to discover that and change your training and your supervision and so on to eliminate those errors. Then he says, after the errors there are the amateurs, the hackers that are just looking. And their methods are so sledgehammer that they show up virtually everywhere, and they are immediately identified and dismissed. Yes we have a firewall that protects us against that, and then when the real red flag goes up, something really different is going on, somebody is really after you, you have the ability to focus on that and focus on it in enough time.

So, without being a salesman, for any of the companies that do these kinds of things, I'll just share with you that that's the experience I've had as I've gone throughout the industry looking at people who try to provide security for a living. And they're the ones who have convinced me that the issue is not privacy, the issue is security. And the role of the government, as it was in Y2K, is not to dictate to anybody how you should solve your problems, not to regulate anybody as to what will happen to you if you don't solve your problem, the marketplace will do that. The role of the government is to try to get as much transparency into the system as we can, so that you can know, with some confidence, the level of preparedness and security that exists in the people with whom you have electronic contact.

I close with the thing I always say to folks who come at me, usually with a little bit of nostalgia, who say, "can't we go back?" In the old paper and pencil days you had absolute security and you were sure the data was deleted when you crumbled up the piece of paper and put it in the shredder. And now, even when you press the delete button, you can't be sure it's gone because they could come along and bring it up off your hard disk and really embarrass you with the stuff you thought you had erased. So, recognizing that we cannot turn back the technological clock, let's be cheerful about it and go forward to solve the problems of security in a world of cyber interdependence. Thanks very much for the opportunity of being with you.