Critical Infrastructure Protection

Peter H. Daly

Peter H. Daly is an analyst, researcher, and writer on a variety of high-level management, public policy, and business issues, with emphasis on information age risk management, economical/financial analysis, and contingency planning. He is currently a consultant with Booz-Allen & Hamilton, as well as a research affiliate with the Harvard Program on Information Resources Policy, engaged in research and writing on issues associated with the effect of global information technologies on traditional national security strategies, and on the global development of higher technology cash-alternative payment systems, such as smart cards, particularly among the less developed nations. Mr. Daly was a senior advisor in the Office of the Secretary of the Treasury from March to October 1998, and served as a member of the President's Commission on Critical Infrastructure Protection from August 1996 to March 1998. He was guest lecturer in management at the John F. Kennedy School of Government, faculty and curriculum advisor at the Center for Business and Government, and an advisor in the Kennedy School/Ford Foundation Innovations Program from 1992 through 1996. He received a B.S. degree in economics from Villanova University in 1963, and later did graduate work at American and George Washington Universities with honors standing.

Oettinger: It's a great pleasure to introduce our speaker for today. You have seen his biography, so I don't need to go into any detail. It's a double pleasure because these days he's become a collaborator of ours on a research project that deals with this complicated set of interactions between the civilian world and the military world, and that's kind of what he is going to talk about.

You know, Pete, that you follow on the heels of Kawika Daguio; the class heard him two weeks ago. General Marsh was going to be here last week, but he got preempted by the U.S. Senate and will follow you instead. So that's the context. All the other speakers are in the military.

Daly: Thank you, Tony. On that note, I am really the second act of a two-act deal here. I understand that Tom Marsh, who was the chairman of the President's Commission on Critical Infrastructure Protection (PCCIP) and did an outstanding job at it, will be here next month. I'm assuming that you have read or seen Presidential Decision Directive (PDD) 63, which implemented most of the PCCIP recommendations, and the President's speech that announced it.

I would like to start out with a very short summary of the PCCIP, and then get into a dialogue with you on some of the key issues involved here. The commission was formed by Executive Order 13010, which was issued on July 15, 1996. The start was really the Oklahoma City bombing, but that was the spark. Underlying that had been a growing concern in the law enforcement and intelligence worlds about the threat of new forms of domestic terrorism, still mainly focusing on bombings and biochemical threats. The mission explains that the commission was set up to do a very broad, wide-ranging vulnerability assessment of the nation's critical infrastructures and eventually to recommend a national policy and a strategy for their protection (figure 1).

It was structured in a rather unusual way (figure 2). It was a private sector-public sector group. There were 18 members, 10 from the public sector, and 8 from various companies that are infrastructure owners or operators. The principals committee was nominally the secretary of defense, attorney general, and the DCI. The advisory committee was chaired by former Senator Sam Nunn and former Deputy

Recommend a national policy for protecting and assuring critical national infrastructures

- Determine vulnerabilities
- Identify threats—physical, cyber
- Develop policy and legislative issues
- Develop policy recommendation and implementation plan

Figure 1
Mission

Attorney General Jamie Gorelick. They appointed eight or nine senior business executives. The steering committee was the deputy secretary of defense, deputy attorney general, and assistant to the national security advisor.

On the left you see something called the Infrastructure Protection Task Force (IPTF). That is basically a strike force housed in the FBI that was set up to react in the event of an infrastructure emergency during the time that the PCCIP was engaged in its work. The work lasted about a year and a half. The report went to the NSC in November 1997.

The commission organized itself into teams (figure 3). I chaired the banking and finance team. Each of these teams performed an in-depth sector security assessment, which involved a lot of contact with businesses, universities, and a multiplicity of government agencies. What we found generally was that a new field of risk had emerged, and it came out of a growing dependence and interdependence of sectors that were traditionally thought of as separate (figure 4). Now, they collectively depend on the information networks. This raised a whole new series of concerns about their vulnerability to attack and natural interruptions. The commission also found that the awareness of these risks was uneven. Some sectors, particularly banking, understood them well;[1] others, such as transportation, did not. The vulnerabilities were growing, and there was a lack of a national focus on the issue.

Recommendations generally focused on the creation of a new paradigm, a new partnership, and new forms of public sector-private sector partnerships centered on information sharing. The commission also recommended that now was the time to act, while the threat was still somewhat distant, and stated that success depended very much on the engagement of the private sector. That basically summarizes what we did.

I think that the most difficult thing we did was define the risk. The factions in the PCCIP were probably predominantly military and law enforcement; secondarily, the intel group; and lastly the private sector people. They really were not convinced of this risk and threat. They did not necessarily see a role for themselves here.

So I guess the first thing we should try to discuss here is the real nature of this risk. Is this a military risk that requires a military response? Is it primarily an economic risk that requires a business response? Or is it a societal risk that requires some kind of decentralized response?

Oettinger: Thoughts, ladies and gentlemen?

Student: My gut reaction is it's a problem for everyone to deal with. The military has a vested interest in addressing the threats and vulnerabilities, but private companies also clearly have motivations for making sure that they can remain operable in the face of catastrophic terrorism in a domestic setting. I guess the concern then—and you spoke to it earlier—would be that the commission currently doesn't reflect enough private industry input into the process, and into the way it went about gathering the information, as well as thinking through some of the policy issues. It just seems like something endemic to a lot of what's been going on, both in critical infrastructure protection and in policy developments affecting areas such as electronic commerce or something like that. Last week Ira Magaziner[2] mentioned that a lot of this stuff seems to be segmented off: you think about it in closed rooms, and it's hard to get people in the media and the public involved in the debate, and to make it lively and engaging. I guess the idea is to remain objective

[1] See Kawika Daguio's presentation in this volume.

[2] From 1995–1998, Ira Magaziner was President Clinton's advisor on Internet policy.

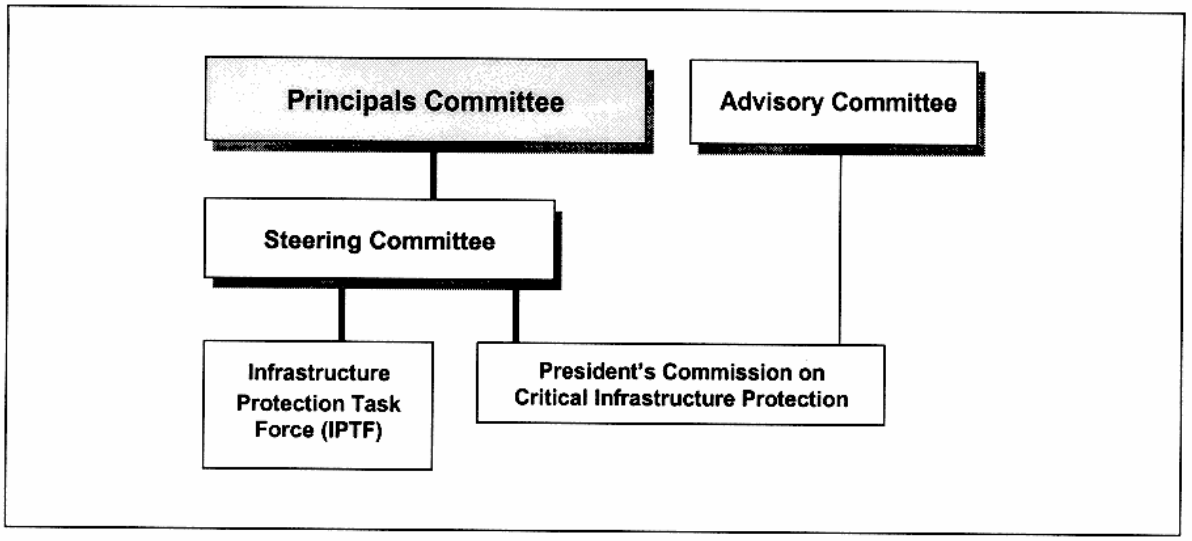

Figure 2

PCCIP Structure

and have the detachment that comes with looking through a military lens and picking apart the threats and vulnerabilities. I don't see where that's been getting anybody anywhere. So I guess we can just open it up now.

Daly: What's the difference, then, between the military and the government role during, let's say, the Cold War versus now?

Student: My impression would be that in the Cold War there was a general focus, to some extent, on industrial planning and seeing the clear links among the economic as well as the security threats and vulnerabilities. Now it seems that a lot of the revolutions in business affairs that we talked about earlier in the class happened away from that industrial complex that the military has been so engaged with; that they're now behind the power curve, not necessarily dictating the direction or even the focus of it. So they're in the position of saying, "Now that we see we're not in the same position as we were 30 years ago, we need the information. We want to create the dialogue."

Student: Two of your slides probably capture at least part of the essence of the change, if you will, in the problem. The threat profile, I think, is certainly one aspect of it (figure 5), and its evolution as well (figure 6). For a long time there were limited capabilities out there, and opportunities weren't that high. We had a good idea of what the threat was. Now it's probably become, to use an overused term, more asymmetric, and the chances of detection are less, and it cuts across all strata of society and agencies in the country. It makes it, I think, a lot more complex and difficult to deal with than it was before.

Daly: It's not so difficult to convince individual firms and agencies and so forth to fortify their own systems. I think they can understand loss and vulnerabilities there. What is really difficult is the construction of the business case for why the private sector should care about the infrastructure generally

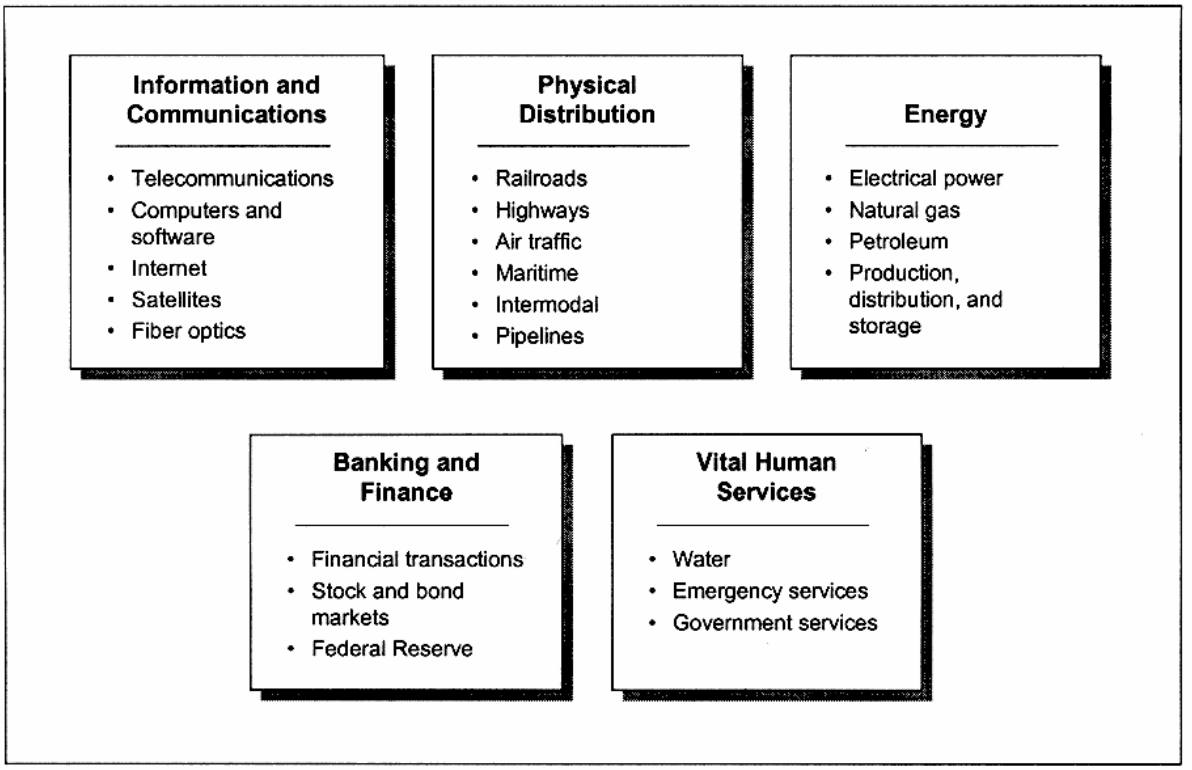

Figure 3

Sector Teams

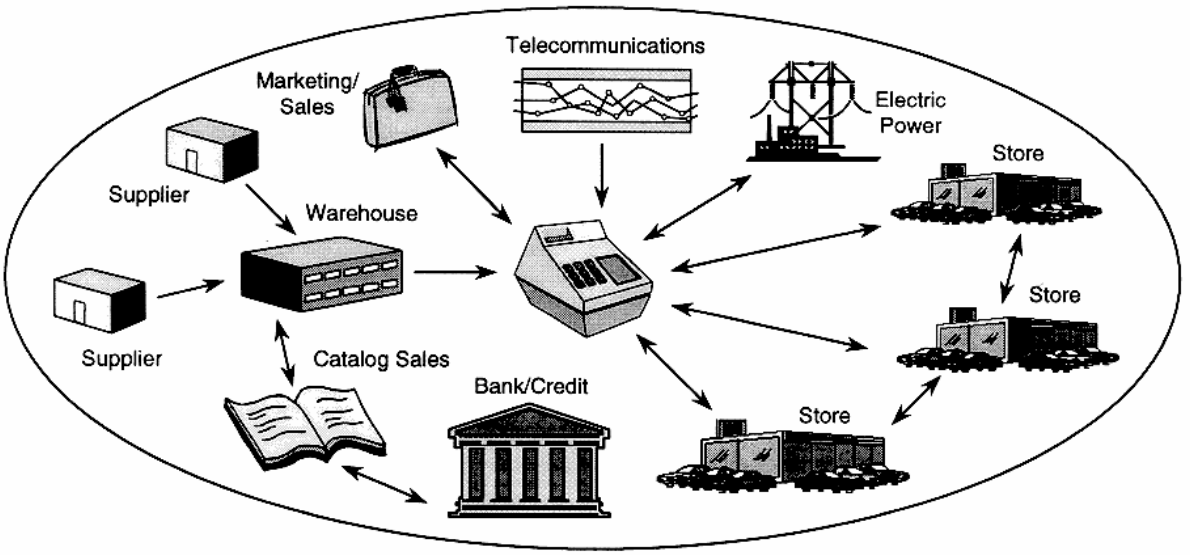

Figure 4

Infrastructure Delivers Prosperity and Strength

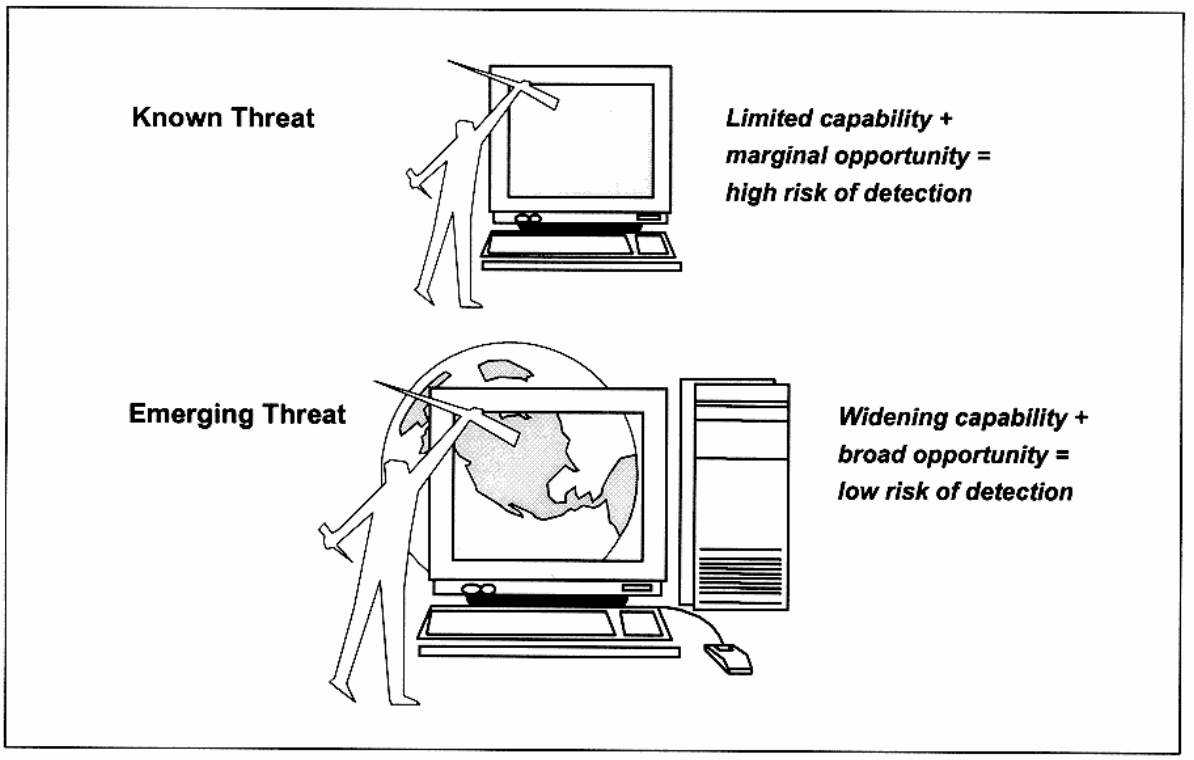

Figure 5

Threat Profile

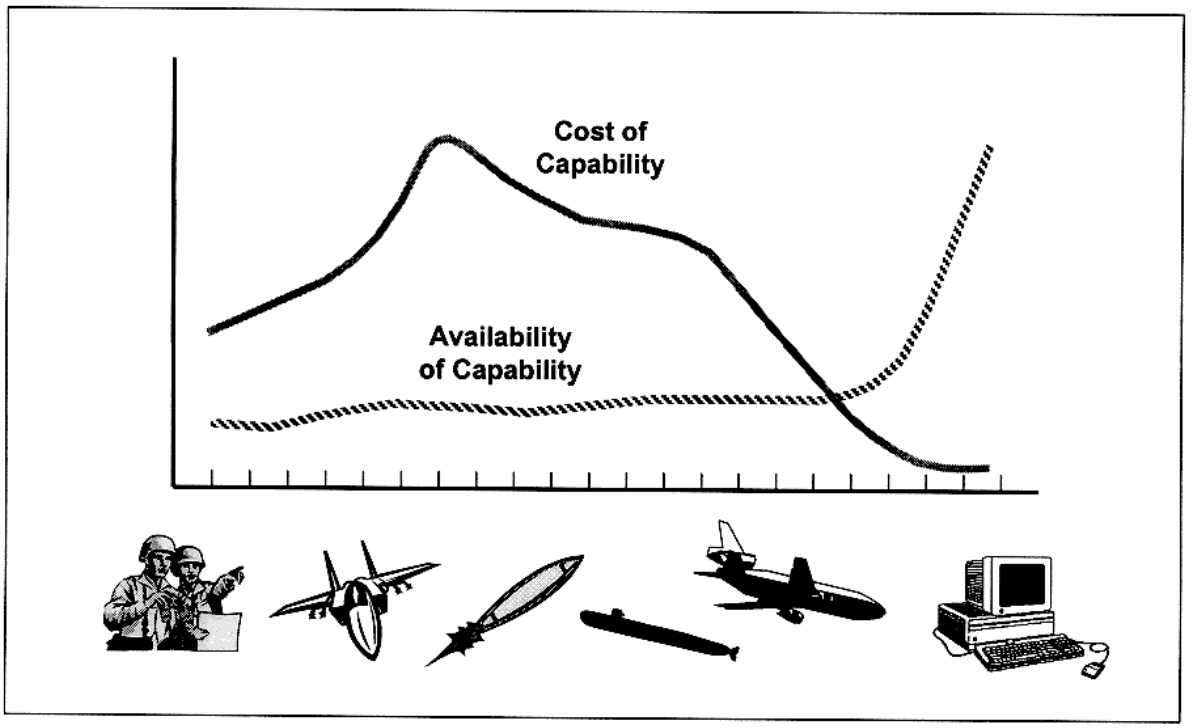

Figure 6

Evolution of Threat

and defend it. Business in the post-Cold War era seems to be in an ascending role, and the understanding of their new role in national security, like it or not, is not well accepted. That's why I ask: "Is this a military risk? Is this something that the military should do or not?" If the southeastern phone system went down, and at first no one knew why, but it turned out that it was an attack by France Telecom on AT&T, what do we do? Should we fire at France? No.

Oettinger: Flood their market with bananas!

Daly: Yes. There would be a business response to it, I think. So, as you say, the interdependence or coupling challenges the effectiveness of the traditional compartments of this whole issue.

Oettinger: May I touch tangentially on a factor that I don't think is causal, but is part of the background? The sharp focus on the Soviet threat, coupled with the fact that satellite, missile, and information technologies were very much nascent and government-developed and -owned resources, provided a situation where there was a willingness to be taxed for defense. There was also a willingness to spend that tax money on what Dwight Eisenhower acerbically called "the military-industrial complex," but it was a complex in which the military side paid the industrial side to do a whole bunch of things. The industry, then, being the recipient of all this government tax money, was supportive of government spending, so there was an engine in which the military and major segments of business were engaged in a mutual back-scratching situation.

It isn't only the vanishing of the threat, or the asymmetry of the threat; it's that in the intervening period, for various reasons including the end of the Cold War, the focus on business and on bringing down the size of the government, which has certainly been a theme through the Carter and Bush Administrations and was taken up by Clinton as well, has created a climate where government largesse to the private sector has dwindled sharply. This is leading up to a question, because despite your words and the commission's words about private sector participation, has a penny been appropriated? Or, in other words, is the private sector being asked to cope with what they would regard as externalities? You said they're sort of willing to take care of their own, only even there perhaps that's limited to "their own" to the extent they can see a business reason for it, not necessarily their own to guard against the threat of a major Iraqi attack or something. Who is paying for things now? Did what I painted make any sense?

Daly: Yes. The report went to the NSC, and the NSC set up an interagency task force, which is mostly a death signal in the bureaucracy. The principal adversaries here were Justice and DOD. Basically, Justice won, and the only agency, the only part of the government, that got any funding and any staff was the FBI. They set up something called the National Infrastructure Protection Center, which is ostensibly a partnership function. It is supposed to invite businesses to share information. Businesses are rather skeptical of this. They don't want to share information, on the contention that they're not going to get anything back for it, and I think they're right. So despite all the talk of a partnership and a new paradigm, it's become, at least for now, primarily a law enforcement effort, with the FBI looking for investigative data, and the resistance to it is very strong.

The only business sector I know of that has started on something is the banking sector. They set up something called BITS, the Banking Industry Technology Secretariat. It's sponsored by the Bankers' Roundtable and has a membership of about 125 banks of various sizes. The American Bankers Association has begun a pilot information sharing process, which was discussed a couple of weeks ago.[3] These are efforts to create private sector-based, sanitized information sharing about cyber invasions and cyber losses. There is a new company called I-Defense, formed by the former CEO of UPI, which is trying to find a niche in this market as *the* voice of the private sector. It is attempting to position itself as the link between businesses and government. It looks good. I-Defense has two major contracts: one with

[3] See Kawika Daguio's presentation in this volume.

Citigroup and one with Microsoft. It is off to a good start, but it's early. So I think the character of the risk is really something new and something yet to be defined.

Student: Does industry really feel itself threatened, or is it complacent in your view? Did they see how vulnerable various pipeline industries are, for example, that run hundreds of miles through deserted locations?

Daly: Industries vary, but I think they generally see their own firms as vulnerable. You don't have to explain it to them. In terms of the connection to the infrastructure generally and the dependence, our findings were that most of the traditional business risk models work on the assumption that the infrastructure will always be there, and that's someone else's job. They are very skeptical about the notion of some kind of a collective aggregated risk syndication method that would involve pooling risk funds. Traditional risk assessment models are not evaluated because there are no actuarial data on losses.

There is an encouraging sign in the insurance industry, which has used risk pooling and risk syndication before storms and that kind of thing, but the extent of an individual firm's liability for downstream losses resulting from poor information security (INFOSEC) is undefined. And so, as I said, an understanding of the character of the risk, the definition of the risk, and who bears it is still in its very formative stages.

Student: It sounds like a classic commons problem, in that a lot of people have an interest in it, but, again, no one has an interest in putting up the initial capital because it's a common good. When you have a market failure, the default setting for that is government. Of course, that has its own set of problems. There are some incremental incentives that probably could be used. I just want to get your read on a couple of them. For instance, you mentioned the insurance companies. Has anyone recommended getting the insurance companies involved to essentially make private industry internalize those costs by paying certain premiums on insurance or setting up some system where government could come in and maybe rate the security—the INFOSEC—and then base that premium on the rating or something like that? I realize there are a lot of obstacles to eventually getting that done.

Daly: There was aversion to regulatory action here, but one that was discussed is a FASB standard. Does everyone know what FASB is?

Oettinger: It's the Financial Accounting Standards Board.

Daly: Yes, it reports to the Securities and Exchange Commission (SEC). There was a move that a FASB standard should be set up to define certain INFOSEC standards for a firm, and if the firm did not meet those standards, there would be a contingent liability on their financial statements. This is something that affects share values, and this is something a CEO would really care about. Again, SEC is so far reluctant to impose regulations on this problem.

Oettinger: FASB, though it's related to the SEC, is in fact in the private sector. It's a privately funded, privately owned organization, so there is some reluctance there as well.

The other thing that seems to me may be worth adding to the portrait you paint is that all of this is happening in a period where the general mood, or at least the rhetoric, is deregulatory, and aiming to get government out of things. The argument is: "I won't do it unless it's for my own benefit, or the benefit of my shareholders and so forth, or unless I can be guaranteed that I get paid for it, or, at the very least, that my competitors are also in it." This is why there is coolness to the notion of regulation or the notion of requiring some kind of insurance. But this comes at a singularly bad time for the set of industries that Pete has been involved in—banking and finance. That's interesting of itself, because those industries are in turmoil regarding banking, and where the boundary is between banking and finance, and whether insurance companies and stockbrokers are part of it, et cetera. So you're dealing with a set of industries where the extent of suspicion among them is exceedingly high.

Therefore, with regard to any question like the one you just raised, even if everybody were favorably inclined in principle, I could imagine a decade or two of guerrilla warfare over the details of ensuring that any regulations not beggar me for the benefit of my competitor within my industry as now defined, or worse yet, within my industry as it might be more broadly defined depending on future circumstances. It's two sets of issues colliding in a state of great flux and darkness.

So in what seems like a very rational setting, there is another element to which, again, I'd like your reactions. A former student of mine is now the head of the Insurance Company Research Institute in Hartford, an institute within the University of Hartford Law School. The impression I get from conversations with those folks is that the insurance industry has over the last few decades been a little bit like the power industry was: sort of sleepy and unimaginative. If this guy is correct, and it's not an industry that is like, let's say, the Internet industries—full of entrepreneurial go-getters—then the idea of the insurance industry becoming proactive in developing whole new product lines and finding a market for them again runs into the accidental situation. Therefore, if you're waiting for initiatives from that portion of the private sector, you're unlikely to get them. So, there is a constellation of interacting complications that tends to provide inertia.

Student: I'm wondering about the question of vulnerability. From a technological standpoint, the Internet is a collection of networks that are connected—there's wireless, there's fiber optics, and some are more physically visible, so a saboteur can blow them up. By contrast, your wireless phone system or your pagers are more vulnerable to natural disasters or to a satellite getting out of whack, which happened some time last year. Is there any view of how the government or the various industries need to address that range of vulnerabilities?

Daly: I think you're defining the Global Information Infrastructure (GII), the wireless satellites, or telecom globally, that does not fit neatly into the traditional kind of home country regulatory structures that vary around the world. It's analogous, I think, to the financial system in that there is now a need, which everyone sees, for some kind of supranational regulatory body that ensures transparency, that ensures interoperability, that guarantees access, and that regulates security and assurances. In the world of information technology, though, most of the regulation and the rules, as I understand it, have come from more or less private sector bodies—the Internet Society and things like that. There has been some government involvement there, but to my knowledge—and I'm sure you know more about it—I don't think it's gotten much beyond the thinking stage at this point.

Oettinger: I think that's fair enough, but for those of you who are interested in this area, there are a couple of places to look. I think you've made a very important point there, Pete. The tradition in the financial services area, over the last umpteen decades, has been for a certain measure of government intervention. If you look at Ethan Kapstein's book *Governing the Global Economy*[4] (those of you who were in my course last fall are familiar with it), you'll see a nice account of how, in spite of what we call "the erosion of the nation-state," et cetera, a principle that Kapstein describes as "international cooperation with national control" works fairly effectively. Essentially the central bankers of the major industrialized nations get together informally in Basel and agree among themselves about certain codes of behavior, which they enforce not through the United Nations or through some kinds of treaties, et cetera, but simply because they informally agree that they will treat any violation they see by using their local instruments, which they already have in place. That's a model that works fairly effectively, although it's limited to the scope of financial services. You can contrast that with the ICANN. What does ICANN stand for?

Student: The International Corporation for Assigned Names and Numbers.

---

[4] Ethan B. Kapstein, *Governing the Global Economy: International Finance and the State*. Cambridge, MA: Harvard University Press, 1994.

Oettinger: ICANN is a concrete example of this grassroots private sector. It's a weird sort of private sector because it isn't the industrial part of the military-industrial complex. It's bearded guys out of various kinds of nerdy universities and small shops and so on who are framing the regime for something that the commercial sector is thinking of increasingly. It's a completely different model of grassroots-upward regulation, evolving in a fashion that is quite different (that's the most I can say at the moment) from the picture you'd see in the financial services industry. So you have another sort of strange coincidental happening, which is that the various pieces of this puzzle operate under very different regimes. The ICANN model and the Basel Accord model are just one example of two intersecting areas, because the Internet is part of the infrastructure of the financial services industry. You have both these influences working on it, but they work on it in very different ways, which even the protagonists don't necessarily understand. It's a very strange situation.

Daly: I take his point, though. We looked at things like tax incentives, in-kind grants, loan guarantees, guaranteed markets, and a range of traditional government subsidies. Beside the reluctance to do them at that time (this was 1996, and the budget was still not balanced and was still an issue), the preferred strategy was government jawboning—basically trying moral persuasion, pardon the expression. It was leadership that way, secondly incentives, and then lastly regulatory action. My own feeling is that industry would react to jawboning mostly from their regulatory agencies. Those are the parts of government that they care about. During the past year, bank regulatory agencies—the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), the SEC—have issued detailed guidance on INFOSEC and made it part of the examination or supervisory system.

Oettinger: Again, it seems to me there is a certain ambivalence. You don't necessarily have to subscribe to the most paranoid theories about regulatory agencies being in bed with their own industries to have a sense that the regulator of one industry is unlikely to want to impose excessive burdens on that industry that might put it differentially behind the eight-ball relative to a competing industry. Yes, bank regulators might do things up to a point to ensure the integrity of banks, but my guess is that if the industry made a case that this put them at a disadvantage relative to, let's say, the brokerage industry or the insurance industry, there would be at least some delay in implementation and some dialogue before anything happened. So again, it's another complication that was not present in the Cold War, centralized, government-largesse-through-taxation model.

Daly: What did you think of PDD 63?

Student: We discussed PDD 63 last week, and essentially it is somehow an ideological digression from the very successful U.S. industry model. Looking back at history, the United States has been probably one of the most successful development models in the last 100 years. This comes about as a result of very decentralized and very liberal thinking on the government's part. Of course, there were particular eras in the history of the United States, for example after World War I or in the Great Depression, where you had very centralized control, a very centralized planning process, in trying to address a particular problem. But when you go into PDD 63, it gives one a sense that you are going to another model in an attempt to coordinate very diverse activities from what is in some ways a very centralized platform. So this is a good way, and certainly this is very reputable in many other places. I think in many East Asian countries this is exactly what has been done, because their societal model has always been that way. But trying to implement that in a country where you are used to a very liberal sense of development may be a bit tricky, to say the least.

Student: I think generally it was a solid piece of work. My only criticism would be that it did sort of happen behind closed doors, and didn't get the play, the input, that it needed. Basically, I think that advocating the best practices out in industry, opening up government, and being sort of in the forefront of creating the best practices and im-

plementing them agency wide is happening and it's good. The directive created the needed thrust for that. It didn't really go in depth, which I think created a lot of debate, on describing the model that it put forth for the Information Sharing Analysis Centers (ISACs). I realize there is a political problem in actually describing what was envisioned with ISACs and how they were going to happen. But it seemed that it created a lot of people turning the wheels and not getting anywhere, because it just didn't give everyone a common base to discuss ISACs. You just know that each industry is going to go off and have a totally new idea of how it's going to implement ISACs, or what ISACs will even do. So I guess it fell a bit short of its promise there.

Certainly, the recent problems the government is having with cyber threats and cyber attacks on some government information infrastructure place the document in sort of a new light, with actual threats now. I think a lot of people are going to go back to it in the coming year and really start thinking about it again. Maybe you have some insight on what's coming next.

Daly: I don't, but I feel that both the PCCIP report and the PDD suffer from a major flaw. Does anybody want to take a stab at that? In fact, these are both very government-centered documents. What is missing from this? All the talk about partnership and the need for new structures, what does it sound like?

Student: I didn't find any benchmarks, anything to measure success.

Daly: That's part of it, sure.

Oettinger: The thing that struck me, particularly about PDD 63, is that it reflects a rather arrogant dimension about the government having things to offer to private industry, which seems completely out of touch with reality. I wonder if you are able to shed some light on what brought that about, because it seems so way out.

Daly: That's easy. What's missing, I think, is any mention of, or any confidence in, the natural market forces that will drive businesses and guarantee that at some point they will understand this risk and guard against it. The reason the report came out that way is the very simple Washington rule. The Justice Department, DOD, and the NSC ran it, and it came out as a government-centric report. It's kind of an old paradigm: the government defines all the risks, tells you what they are, and then expects you handle them.

Oettinger: It seems to be so anachronistic.

Daly: Yes, and I don't understand fully what became of this whole market-based idea, because, as you say, this does not seem to fit into contemporary thinking.

Oettinger: For those of you who heard Magaziner, did he have anything to say about this?

Student: As soon as you started talking about the market and possible incentives, politically it would be explosive. You can't have a PDD that begins to address new tax incentives. Congress would just throw their hands up. That clearly oversteps the lines of executive powers.

Daly: It's silent on the whole market forces point. You don't necessarily need tax legislation. But there are natural market forces that will eventually drive businesses, for their own survival, to invest here. They may under-invest, but they ultimately will invest if their risk is real.

Student: This question was raised before, but it just strikes me and I'm trying to understand it. What would be the mechanisms for coordination between all these centers, councils, and offices? What is the link between them? What is controlling all of them? Are they all really necessary? Will they compete, or join in some way?

Daly: The commission proposed a very complicated national structure. Essentially, each sector would be coordinated by a lead agency. For example, the Treasury was named the lead agency for the banking and finance sector, and the Department of Transportation for the transportation sector. Their

job is to reach out, organize that sector in some fashion, set up ISACs, and get that system in. It's a stretch.

Oettinger: Just as a few minutes ago Pete pointed out that the appointment of an interagency coordinating committee is a signal of distress, the notion of a lead agency strikes me as an ill omen. Again, I'd like your reaction. Bringing that into the context of this particular course, the National Security Act of 1947 created the Office of the Director of Central Intelligence as the focal point, the coordinator, of all U.S. government intelligence activities. Fifty years later, the Community Management Staff and the Office of the Director of Central Intelligence, as opposed to that individual functioning as director of the CIA, remain something of a bad joke in that the money is elsewhere. You've heard this from some of the speakers here. When you see "lead agency" or "coordinating agency" in the U.S. government context, you have to interpret that in the light of that kind of history that says, "Aha, this is a good bureaucratic way of putting a label on something that will probably make no practical difference except for a few officials who, once a month or so, have to meet somewhere and do something." So that aspect strikes me as not only hollow, but also counterproductive.

Daly: I can't imagine that John Reed, the CEO of Citigroup, would call somebody called "sector coordinator" to report it if they were suffering from some kind of cyber attack or thought they were. He's going to call the president of the New York Federal Reserve Bank. He's going to call Secretary Rubin, and people like that. This is a creation that doesn't fit into the reality of the marketplace. I think at best it's a real long shot to succeed.

Student: I was actually doing a comparison of how much government should intervene, and I compared different East Asian models to the model of my country, which is Kazakhstan. The case I ran into was the SEMATECH project, when the United States fell so far behind in semiconductors that they decided to take the Japanese model and to intervene heavily in the market. The result was SEMATECH, Inc., where DOD paid for half of the investment, and invited a lot of other companies to come in, basically to pull up from the back. Many computer industry analysts believe that push really helped American chip manufacturing to gain back the market or some share of the market. In that case, the industry was really under threat, and that threat was obvious because if U.S. computer manufacturing fell behind, it would have real implications for the U.S. military and for national security. So I think there is no real threat at this point, but as soon as industry feels a threat, there will be much more welcome for the sector approach, and they will call that interagency person faster than they do it right now, because at the end of the day, when things go bad, you people turn to the government if there is nobody else to turn to.

Oettinger: Our program did a study of consortia that bears out what you say. I'll give you a copy of it. It's by Norm Zimbel.[5] The mission of SEMATECH was fairly sharply focused and narrow, and occurred under well-understood conditions. The contrast, which is outlined in that study, is MCC, the Microelectronics Computer Corporation, which kind of went nowhere because the circumstances were much more like the ones you're describing with the PCCIP. There was this vague feeling that something ought to be coordinated, and there should be some kind of joint collective enterprise, but the players mistrusted one another, and nothing much ever happened. So you're making a very good point.

Daly: A basic finding was that there is no national focus on this. Some of the agencies involved felt that there was "no one in charge," which they thought was a major flaw.

Oettinger: Let's dwell on that for a moment, because the tendency when something like that is found is to say, "Let the President do it." That tends to be meaningless. If you

---

[5] Norman S. Zimbel, *Cooperation Meets Competition: The Impact of Consortia for Precompetitive R&D in the Computer Industry, 1982–92*. Cambridge, MA: Program on Information Resources Policy, Harvard University, 1992.

look at a list of all the things that the President of the United States is supposed to do under statute or whatever, there's not enough time in anybody's life to do all of them in a meaningful sort of way. What does a "focal point" mean for something that encompasses damn near every aspect of the infrastructure, which is damn near everything that matters? The notion that somehow you have a focal point for everything that matters seems self contradictory, which is why it seems to me that Pete's point that market forces have been underrated and ignored in this is so important. The merit of an unfettered market is that in hellishly complicated situations the invisible hand is more likely to produce better results through individual initiatives than some hypothetical, centralized, all-seeing, coordinating something-or-other.

Student: The other case I ran into was the U.S. steel industry, which says, "Please don't get into our business. We'll do it the way we want to; the market forces will solve it." When Brazil or Korea or Russia start dumping, they turn to the government and say, "Please put in some quotas." That happened in the past, in the 1970s. The steel industry did not coordinate, did not invest much in R&D and in research to make their own industry competitive. So I wouldn't trust the invisible hand so much because at the end of the day, again, it is taxpayers' money that would have to be spent because the consumers will have to pay higher prices for the same services.

Daly: Yes, and there are very real qualitative differences between the way the public sector sees risk and businesses see risk. The government's timeframe generally is longer. They're more concerned with loftier and broader concepts. But still, I think the PCCIP and the PDD 63 proposals are a rational attempt to simplify and to stabilize a very complex and very dynamic set of conditions. For that reason, I don't see it as being effective in the long term.

Student: Maybe government did not provide enough incentives to show that these are the circumstances that you run into, or maybe the circumstances are very difficult to describe. They cannot really prove that Citigroup will lose a given amount of money if something were to fail, as opposed to the competition, which is very small.

Daly: The theory is that the government will share information or intelligence with corporations, which will then put it into their traditional risk models. They will change their models. They will show that investment is necessary, and they will make that investment. I think that's a stretch.

Student: It sounds as though it really did have great expectations and really tried to attack the problem. To some extent though, they really missed the boat in the sense that you need to start incrementally. It's like balancing the budget. You don't expect it to happen immediately; you've got to think about the long term and go from there. So, with that in mind, what would you say would be that first incremental step if you were going to go back and rethink PDD 63 and PCCIP? Do you have a quick read on that?

Daly: Honestly, I don't know. As I said, I think the strategy needs to incorporate more respect for market forces and for the natural survival instincts that businesses have. For the revision of the PDD 63 and the PCCIP report and so forth, I would see a government role and a revisiting of the national compartmentalized structures that we have. I would also see a much stronger emphasis on, and a much more encouraging statement about, the private sector's capability to recognize this risk and respond to it.

Oettinger: The basic attitude gets in the way. This is now referring to the presidential directive rather than the PCCIP. If you have a bunch of people who believe that the government knows it all and has something to say to the private sector, you're not going to get even any thinking done about ways that you can reverse that flow. For instance, going back to Daguio's presentation, you could say, "We in the banks have a much better idea of who's after our information and our accounts and so forth than the police or the FBI or the military do, but we're reluctant to share it because of antitrust considerations or

creating a run on the bank or whatever." If you buy that argument, then you do things like provide antitrust immunity under certain circumstances. You propose legislation that would protect the industry against improper disclosure. One of the ways that the Commerce Department and Treasury Department get financial and economic information (and census information, for that matter), is not only by guaranteeing confidentiality, but also by having on the whole a pretty good track record over the decades at enforcing it. They leak occasionally, but overall they've been fairly reliable. There's nothing like this in this area, and there won't be unless the pieces of the government that handle this change the direction of the flow.

Daly: There's a possible model in the world of finance. It's something that was set up after the 1987 market crash, and it's called the Financial Markets Working Group. It's deliberately loose and informal. It's chaired by the treasury secretary, and its members are the chairman of the Fed, chairman of the SEC, and chairman of the Commodities Futures Trading Board. Below them are a series of regulatory agencies and specialists of various kinds, and then under them is this complicated, large network of investment banks, brokerages, and money-center banks. When an event occurs, as in Asia or Russia or Mexico, this group forms, and it talks, and it decides what strategies to follow—what the government needs to do in a sense—and then after the crisis passes, it goes back into being a very loosely structured entity. That might be a model. Instead of looking at rigid, bureaucratic roles and functions, assignments, and permanent staffs and all that, this might be a good way to look at a very flexible, fluid, really unpredictable situation and manage it as a risk management function instead of having to kind of preselect your responses.

Oettinger: But, if I may draw you back to something you said earlier (and correct me if I misheard you), it also builds on the fact that there are government agencies involved in this informal process that do have statutory, regulatory authority. Therefore, there is a necessary and ongoing relationship, not only *de jure*, but also *de facto*, at all sorts of levels of management that this whole thing can draw on. So that is indeed a potential model, but it doesn't necessarily address those parts of the infrastructure where there is no current regulatory apparatus. Any thoughts on what might be doable in areas like that?

Daly: Take the example of energy. After the 1993 or 1994 outage, when it was threatened with regulatory action, the electric power industry formed NAERC, the North American Energy Resource Council. This is a purely industry coalescing of firms to ensure that there is sufficient capacity and redundancy in the system, even as it moves toward a deregulated model where they go away from reserve capacity and more to a just-in-time model. This apparently has functioned well. So this is a case where fear of regulatory action kind of moved them to form this council.

Oettinger: And some highly visible incidents.

Daly: And some embarrassments, of course.

Oettinger: Do you have some other thoughts on this?

Daly: It's interesting to look at the differences between the way the public sector, the government, looks at risk and the way the private sector does. Government tends to look at risk in terms of national security, economic security, public good, political advantage, popular support, things like that. It is the way, I think, that policy officials tend to gauge danger. The private sector obviously tends to look at financial risk, earnings, share values, and so forth. They look at competitive advantages and losses. They look at operational risk, which involves the capacity actually to bring a product to market, or quality risks that would damage their firm. They look at reputational risks in terms of popular support, customer loyalty, corporate image, and so forth. So, when you talk about partnership, they kind of miss each other. People in government look at risk entirely differently, I think, than business people do. Their time span is different. Their scenarios, upside and downside, are different. Their planning

mechanisms are different. Their measurements are different. Their benchmarks are different. So this is, I think, a very big, central issue here when you begin to talk seriously about a partnership: the two major parties are coming from very different starting points. Of course, one of the fundamental prerequisites of a partnership is a sharing of goals, and it's not entirely clear that the public sector and the private sector share goals here.

Oettinger: Have you any thoughts about how you reconcile or build a bridge?

Daly: Not yet.

Student: It's a contrast to your earlier example with NAERC, and just realizing how ineffectual it is in reality. Being a voluntary organization with no legislative teeth, its ability to indoctrinate private industry in a longer-term risk management scheme hasn't really been working. Then they're monkeying around with new agencies on top of that, and it seems like it's a real quagmire in terms of getting anything done. To some extent, if you can move beyond just the risk of it, it seems that what really is necessary on government's part is to think about some real goodwill gestures. I'm thinking more in terms of the policy dichotomy in saying that we need to foster more INFOSEC, but at the same time preventing the implementation of robust encryption and stuff like that. It's an interesting example, and I know that's an issue that probably needs some time to develop, but does that seem reasonable? Or, if not, what will be the drawbacks? I guess it's the goodwill or "great white fleet" kind of mission for government and private industry.

Daly: I think the best gesture of that kind would be serious sharing of information, or intelligence, which is a very complicated matter. Law enforcement sharing information with industry pools is not there now. There's a great reluctance to do it. Some of it has value, some of it probably doesn't.

I think the theory that government should seriously share critical information about threats and vulnerabilities for industry to use in its risk models is a respectable one. I think there is a good chance that if it were truly done as a first step, as a gesture of sincerity, it might evoke a change, or even evoke the kind of industry response that the PDD seems to want, but, in effect, doesn't want to buy.

Student: Could you maybe hypothesize about the types of information that would be necessary? I know, for instance, that the CIA collects a lot of information on foreign hackers and stuff like that. Would it be focused in that realm or would it be just general, best practices kind of information?

Daly: No, focused on specific emerging threats and events. That's very difficult, though, because, first of all, a lot of it isn't certain. It's speculative. Second, if you share it, whom do you share it with? Do you share it with all firms or just some? If you're sharing with just some, aren't you giving them a bigger edge? So it's a complicated matter. But I think the starting point to engaging business is finding some way—structuring a way, experimenting with a way, piloting a way—to share sensitive threat information directly with the targets, and it isn't done now. It's done sometimes, but not on a regular and reliable basis.

Student: Are any other countries taking an initiative on infrastructure protection? I'm thinking in terms of nongovernmental organizations. Maybe another country would be the leader in getting one of those organizations to start driving industry in this country.

Daly: Not really.

Student: I would say that some of the European countries have looked at this problem for a long time, and looked at it quite differently than we have. Maybe it's a matter of geography, if nothing else; just sheer size. I was an exchange officer with the Italian Mountain Troops for two years back in the late 1980s. When Desert Storm happened, they had soldiers who were assigned to very sensitive points throughout the country: electrical power plants, anything that from an infrastructure standpoint could cause damage or could disrupt life in the country. It was pretty darned organized, and that was a good 10

years ago. It wasn't all that sophisticated, but it was certainly pretty well planned out considering the capabilities they had. So other folks have been dealing with it. Part of our problem here too is our culture. In some aspects we're seen as being very transparent as a society, and whatever moves it would take to mobilize any forces on a large scale, I think, would probably be fought unless we really perceived the threat to be imminent and pretty clear. So that makes things a lot more difficult, just because of the culture we come from as Americans. I think it's harder to deal with.

Daly: In Japan, MITI (the Ministry of International Trade and Industry) is now dealing daily with this too, forming partnerships and things, I think.

Student: One thing about the PDD I think is at least positive. I've seen some directives in the past that just provide guidance, if you will; they just say, "Go forth and do this," but there is no agency or no specific organization or person who has some accountability for the process. At least in this particular instance, even though it may add to the bureaucracy, there is some structure now that says *you* are responsible, *you* are accountable for making this happen. I think that's probably positive.

Daly: Yes, sure.

Oettinger: The cynical view is that it gives the appearance of that without the reality. That's why I'm skeptical. We won't know for a while.

Student: Right. I would agree.

Oettinger: Am I being excessively cynical?

Daly: No.

Student: I would think there is some common ground. Certainly there need to be other market forces and some sort of incentives for private industry. There's got to be some common ground out there so that we can at least make some headway initially.

Oettinger: Let me challenge you, Pete, on something that seems to be an assumption of yours, which is that the image or the reality of government-private sector partnership makes sense. Your folks have been directed toward making it real, but accepting the principle. One of the reasons why government exists is to handle things that cannot be done by the private sector. We delegate authority for certain purposes. Now, suppose that you instead set it as a task to identify those things that are most appropriately done by the private sector, and those things that are most appropriately done for the common good by government—by taxation, by fiat, and so on—which is why we delegate authority to government in the first place. What justifies this notion of partnership? Can you give us a sense of how we got into that, and why that makes sense?

Daly: My view is that the only reason partnership became such an important part of the PCCIP report is that in fact the infrastructures are private assets, and the government is restricted, naturally so, in its capacity to manage them. A partnership is the only option. I believe it was discussed in entirely simple terms and, as I said before many times, does not really take into account the way the market works for these companies, particularly in a time of globalization and new regulatory regimes and so forth. You cannot approach the partnership using the traditional models from the past. I think that's what's missing here, because it is a real new paradigm, if you will, of a partnership that has government setting a structural framework, but the actual management and defense of the infrastructure remain primarily a private sector function. Does that respond to your question?

Oettinger: Yes, and it still nags me. Despite a lot of pretense, there are a lot of open-ended questions here.

Student: I guess my feeling on partnership may not be in the same vein. It would be that partnership implies mutual benefit, and it implies a sort of consensus. Whenever you have a very weighty problem, and you try essentially to attack it through a consensus, it's like a race to the bottom where you get a very

marginal solution, or it doesn't optimize all the parameters. What it really lacks is leadership, and by its very nature, when you have a leader, it's not necessarily a partnership anymore. It becomes a hierarchy that essentially puts the partnership in the back seat. I guess that speaks more to the theory of partnerships and coalitions and stuff, which we read about. Do you have any thoughts on that?

Daly: A partnership, to be effective, has to feature enforceable commitments, which means there has to be some way to make them work. Frequency of contact isn't necessary. That was Tony's point about the Financial Markets Working Group: that there are regulatory agencies that have regular in-depth contact here with the private sector. There probably has got to be a pure and sincere recognition of mutual interests and agents, and I'm not sure those exist right now in this field. I think it's more characterized by skepticism and resistance. I'm not sure government fully respects private sector interests and vice versa. Contacts, with the exception of the regulated industries, are stilted and focus mostly on events of various kinds. The commitments are enforceable, to a point, in a court. So, I think the basic elements of a partnership are not there yet in clear form. I think they are there to be found, but they are not apparent yet.

Oettinger: Let me try a wild idea. Maybe the basic thing that's lacking is consensus on what's to be done. I'm wondering now whether the partnership thing isn't a smokescreen (not deliberate), because if there were consensus for partnership, then presumably that same consensus would operate in the political realm. As long as there is consensus, whether it's labeled a partnership or it's labeled legislative action or coercion or whatever, the label matters less. Isn't the issue then really not that there is somehow a mechanism that's lacking, but that what's lacking is a substantive grasp of what needs to be accomplished? Is that a sensible statement, or am I missing the point?

Daly: There's an inertia, and then there is the fact that a lot of powerful interests like things the way they are now. I think back to 1993 or so when the administration made a proposal to reform bank oversight. There are four bank regulatory agencies—the FDIC, the Office of the Comptroller of the Currency, the Fed, and the Office of Thrift Supervision. The secretary of the treasury at the time was a former Senate Finance Committee chairman. There was a democratic President, a democratic Congress. You would think this would be a very logical thing to do. These are four agencies that are now doing separate jobs and it's not strange for a bank to have three or four agencies there at the same time, and it's a messy situation that dates back to 1934, et cetera. Well, it was dead on arrival. Why? Because banks like it this way. So, just because it's logical and makes sense doesn't mean that it's possible. The partnership falls in the same realm.

Oettinger: We are nearing the time when we have to conclude in order to vacate the room. So let me thank you for a very interesting and challenging set of ideas. We have for you this small token of our large appreciation.

Daly: Thank you. It's been very nice. Thank you all for your kindness. I appreciate it.