INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Infrastructure for Security
Nina J. Stewart

Guest Presentations, Spring 1993
Barry M. Horrowitz; Randall M. Fort; Gary W. O'Shaughnessy; Nina J. Stewart; Walter Jajko; Edward D. Sheafer; Michelle K. Van Cleave; Jerry O. Tuttle

August 1994

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-12-7 **I-94-5**

An Infrastructure for Security

Nina J. Stewart

Nina Stewart is Executive Assistant to the Director of Central Intelligence. From September 1991 to February 1993, she was the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures), Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence. Her career has included positions as: police detective and head of a narcotics unit; special agent with the State Department; State Department Olympic Security Coordinator for the 1984 Olympics in Los Angeles; Staff Assistant to the Secretary of State's Advisory Panel on Overseas Security; Staff Assistant to the Moscow Assessment Review Panel; Counterintelligence Officer; and Executive Director of the President's Foreign Intelligence Advisory Board. She represents the Defense Department on the National Security Telecommunications and Information Systems Security Committee, and she chairs the Intelligence Community's Advisory Group for Security Countermeasures and the National Industrial Security Program. She received her BS from Abilene Christian University, and has completed one and a half years of the JD program at George Washington University School of Law.

Oettinger: This brief introduction is absolutely necessary. Since we got Nina Stewart's biography, she has a new job, and is now the executive assistant to the Director of Central Intelligence (DCI). I want to add one other more personal remark: it is an enormous pleasure to have her here, because at one time I worked for her. I relish the opportunity to welcome her to Boston and to have her with us at this seminar. Nina, it's all yours.

Stewart: Thank you. I didn't have any particular prepared remarks today, so I thought we would make it a very informal sort of discussion at Tony's instructions. But I did want maybe to kick off the session by talking about and considering something that is near and dear to my heart, and near and dear to the Director's heart: that is, how we go about making some fundamental changes in the whole security infrastructure of our business, so that (1) we are more efficient, (2) we can reduce cost drastically, and (3) we can improve technology by allowing information to flow more easily from government to private sector and vice versa. Having said that, I just want to give you some snapshots of my own personal opinions on what is wrong with the current system that we have in place in the government, and what we might do to reopen some of these issues and look at other ways to do business.

Our whole security infrastructure was developed, as you know, during the Cold War, and it was really developed to satisfy customers in the industrial age, not the information age. Some of these policies and procedures were developed 30 or 40 years ago. It's not that we haven't been well served by them; we have. But none of this was really developed in order to allow us to share information at the gigabit level the way we do now between organizations and between governments and between nations. It wasn't developed to allow us to integrate warfighting components. It wasn't designed to integrate the UN kind of arrangement to share information. So those are just some of the factors from the government's standpoint.

From the private sector perspective, there's the compartmentation of our programs, and some of them very much do need to be compartmented. During the 1980s there was a kind of explosion of compartmented programs. There was a lot of money to do that. Compartments did expand, and one of the questions that we have to ask ourselves is: were they expanded, or was the program created, because it was really necessary to have that tight security control, or was it maybe to prevent some scrutiny from whomever? So that's one of the things that we look at.

My thoughts, as I have been talking with Secretary Les Aspin and Deputy Secretary Bill Perry of the Defense Department, is that they've all linked arms and come to the conclusion that we do need to do sort of a zero-base review of our policies and procedures and come up with some new suggestions and new ways of doing business, to move away from what I would characterize as whole total risk avoidance. Policies were developed in order to completely avoid another Edward L. Howard or Ronald Pelton, and everybody who came into government has gone through this rigorous process in order to prevent those kinds of spy cases. We still have to maintain security procedures so that we can be relatively assured that we have good safeguards in place and that we can find those kinds of problems. But at the same time we need to be able to attract people into government, and keep people in government, who maybe do not want to join us because they don't want to go through the processes and procedures that we now have.

I would just say from my own experience that all of these different disciplines in the security field were carried out separately. Personnel security issues were dealt with differently, in their own separate fashion from physical security, from technical security, from information system security, from operational security, and from counterintelligence as well. There has been, in my view, a lack of integration. For example, I've had numerous defense contractors talk to me about 400 inspections that they had in one year by all the different components in the government basically reviewing the same sorts of things. I've had them tell me that they built a secure room for a particular program because (I am not going to pick on anybody), let's say, the Navy said to build it to this specification, and then the Army came in and said, no, that is not what we want, we want it to this specification. So they may have spent millions of dollars on this particular enclosure that they may never use again, and I'm not talking about little enclosures here; we may be talking about an airport style of building. So, those are some of the things that hit me when I was over at the Defense Department, and also now in my new job.

Oettinger: Are you about to move onto something else? Because I am about to ask you a question on this before you go on.

Stewart: Go ahead.

Oettinger: One of the crotchets I'm exhibiting in the class here is to try to relate everything in terms of the whole. What you just described reminded me of a private sector incident that I was witness to many years ago in a bank that had new computers and was trying to be very secure about its data processing, et cetera, et cetera. It had a very fancy double lock access kind of thing, where if they didn't like you inside the first gate they would close the second door and there they would gas you or something if you didn't pass muster. There was all this fancy stuff . . . , and then they would take the day's worth of punched cards (that will help date it for you) and put them in the trash, and anybody who wanted to get their deepest secrets would just come by and collect the trash. Meanwhile, access to the computer room was almost nil.

Now, this protection of turf — left hand, right hand — had nothing to do with government. The folks who made the double locks and the folks who did trash have no idea that either that one or the other exists, or that they have anything to do with one another. It's odd. I'm wondering, how much of this within the government has to do with old-fashioned organizational bumbling, and how much of it is specialized due to the particular nature of the security problem. Do you have any sense of what we are dealing with?

Stewart: In the Department of Defense I tried to get my hands around the money aspect of what we spend on security, because there were no budget line items. I had a study done by IDA (a private firm) and they concluded that, throwing out the special access programs and some of the other issues that we simply couldn't put our hands around, the Department of Defense spends over $6 billion on security programs. Now, that's a really conservative figure, so let's double that. We are not talking about loose pennies here. We are talking about big dollars, even by Defense Department standards.

Oettinger: "A billion here, a billion there . . ."

Stewart: Yes, "pretty soon we're talking about real money"; that's right. But I'll give you an example about how the disciplines differ from one another. All of us sitting in this room would be cleared to varying standards if we belong to different agencies. I've worked for four agencies now, and on each occasion my whole security background investigation, which some agencies spend a lot of time and money on, wasn't accepted by the next one. We went through this process over and over. My neighbors think I am a spy, because they would get contacted so many times. These kinds of things, the redundancy in the system, I think are something that can be fixed.

Another long-standing example is in the physical security arena. There wasn't much creativity in the technology that was brought to bear in physical security. For example, old mechanical locks on safes, has everybody seen these? They have been around many years. Partly because of the leadership of the Defense Department, the physical security experts knew that they needed to get on with their technology, get some new locks, and so they developed an electromagnetic lock with a certain firm. It is a super-duper thing and it's more secure than the existing lock. The problem was that the Defense Department has just arbitrarily said, "Okay, we are going to replace all existing safes and locks within the block, wholesale." It didn't take into account that some of these safes were sitting in the middle of a SCIF (secure compartmented information facility) which was sitting in a guarded building, which is alarmed, and has other rings of security around it. None of that sort of consideration was taken into account, and that's a several-billion dollar effort. Those are the kinds of things I'm saying that we need to think more rationally about, and not just wholesale and myopically pursue these particular areas.

Student: But, going back into Tony's point a little bit, then you have to have: let's improve the physical security for safes, and then on the other hand, we'll put in these new computer systems that have no security in them and then put the safe data on them. Then you go from a totally different direction, and the coordination between different branches, as Tony said about the bank, just isn't there. There is no coherent picture of "this is what we need to do to bring the basic level of security of everything up to whatever is the appropriate level," and do it from a coherent framework as opposed to an ad hoc framework.

Oettinger: There is a problem here that is even worse: the intelligence that nobody wants to own. We've had a number of discussions about the orphaning of intelligence this semester. It appears this is not even intelligence. The line manager will be the commander, or something, who gets something positive, like where is the enemy?

The security is a little bit more like buildings and grounds. It is something where it is not quite clear what it does for me. So I probably have a double whammy in getting interest by the folks who are normally in power, whether it is in corporate entities or in the military, to focus on it. Is that what we might guess? From your more direct experience, is that a reasonable guess, or is that armchair nonsense?

Stewart: No. That is, of course, an example too, where you talk about the lack of coordination. Let's take the counterintelligence arena. Counterintelligence, particularly with the FBI, and with DOD, and to some extent with the CIA, is separate from the positive HUMINT collection. So, many questions arise if, let's say for example, the GRU (Russian military intelligence agency) becomes more active and aggressive from the counterintelligence standpoint, and you see much more going on. So as the threat assessment of that activity from a counterintelligence standpoint you'd say, "Those guys are just bad guys. They haven't stopped, and we've really got to do something about them and, by the way, Yeltsin probably supports this, too." I'm not sure that takes into account other questions that affect intelligence as a whole and that's the answer. What is the relationship between you and the leadership? Is this a rogue sort of effort, is this a rogue GRU effort, or is this something that's government sponsored? To what extent do we, ourselves, encourage that by running double agent operations? So there are a lot of other questions that I think need to be answered, and we need more of a melding of positive intelligence from a counterintelligence standpoint. Those are just some examples.

On the classification management side, I think it's probably true that we have a tendency to overclassify, that we've not managed the process well enough, that we tend to delegate the classification authority to, say, the secretary in our office, and that there's no real effort, once it's classified, ever to declassify it. That just is too hard to do. So we have this burgeoning classification of data quantitatively increasing over the years. There's the whole issue about the technical security area. We spend billions

and billions of dollars to shield our buildings and our rooms from electromagnetic collection, TEMPEST collection, and yet I think it's fair to say that in the United States we neither have enough information to make adequate judgments about whether that was necessary, or we didn't collect that information. We tend to assume an attitude of "If we can do it, they can do it," and then we juxtapose that position by saying, "We're going to protect this because that's what we would do in that environment." What I'm trying to say is there was never an intelligence collection effort to find out from the security countermeasures side what we ought to be doing. I'm saying this in a broad, general sense. There are obviously some exceptions to that, but not many.

Oettinger: Let me stop you there to ask you a question, partly drawing on your background way back as a detective, because I'm inclined to disagree mildly with what you just said on some of this emission stuff. There was a period — and I'll finger the late Ford Administration particularly, because Nelson Rockefeller was deeply involved in their public traces — of Rockefeller's pronouncements on the Soviet's interception of U.S. communications, and vans traveling around the country and so forth. So it isn't as if it were happening in a complete blank. My guess is that instead, there's an old Yiddish saying, "For instance is no proof," and that may have been ignored. For instance became a proof of a vast kind of thing, but to make a thorough study, to assess magnitudes of something as opposed to for instances, would require mounting a fairly heavy effort. There's got to be some budgetary concern. You can't go looking for everything.

Stewart: No, but I think that some commonsense standards are necessary. Some of these requirements were out of scale. I'm not talking about mounting a major effort. Some of these requirements could be asked of defectors and put on the list of questions to be asked of this mass wave of humanity that came out of Eastern Europe these past several years. That's all I'm saying. I'm not saying you necessarily have to mount an effort. You simply ask the question. There's so much information coming in now that we are awash.

Oettinger: Over a long period . . . or not doing it.

Stewart: Right. We talked about the different standards from the different agencies. The criticism of our personnel security is it takes too long, and somebody can be cleared by one agency and go to another agency and be found not suitable. I think that if they're working on sensitive programs with one agency and you have a common security background investigation, which the President signed off last year, then it necessarily follows that we ought to have some common standards by which to adjudicate people in the intelligence community.

Student: Do you support the lie detector as a way of doing that?

Stewart: I'm going to defer that. The reason I say that is I think that you showed me what you think about it by calling it a lie detector. I can't think of a single person who really likes to submit to a polygraph. If you know of someone, you let me know. The polygraph has been, as you know, an instrument that has been used by several of the agencies for 40-some-odd years. I think it's fair to say that until relatively recently, let's say the last four or five years, there was little to no research done on the polygraph; not just countermeasures, but improvements and that kind of thing. Then there were several surprises in the intelligence community with this instrument, and then you have a different kind of effort, but I will tell you that my boss feels very strongly that this is an issue that he wants to review.

Student: Just a little more on the polygraph. Different agencies utilized polygraph differently, and each agency has a reputation for doing a lifestyle polygraph, whereas DOD generally does not do that. Is that one of the things that will be reviewed?

Stewart: It's also something that influences the standards by which a polygraph is employed. Standards mean questions, and how it's used, and at what point it's used, and the like. There are different standards for training. Some of the polygraphers go through one set of training procedures and I'd say this is another of CIA's problems. Does somebody else have a question before I launch off into another tirade here?

Oettinger: No, I think we'll let you go on.

Stewart: Okay. I'd also say in the personnel security area, not only has it been too slow and we have different procedures and different appeal procedures, but also we tend to focus on the front end, when people first come to work for an agency, and most of the studies of convicted spies or spies who have been caught have shown that they didn't start out or come in to spy. Somewhere along the way they made that decision, but it wasn't when

they first entered the agency. Of course there were a few plants, but mostly people decide to spy for various reasons while they're employed and there is not enough focus on what I would call continuing evaluation, rather than front-end evaluation.

I think I mentioned it before, but these questions that I've been talking about are some of the issues that the Director of Central Intelligence wants to grapple with, as does the Secretary of Defense. So I think that in the next year you may see some major changes coming out of the reviews of this nature. Dr. Perry has given several speeches already where he talks about the budgetary costs of these procedures and the fact that we need to review some of our basic assumptions. My boss has given countless talks, both publicly and to the President, about how he wants to review this infrastructure cost and see if we can't make some significant changes. So I want to throw out those issues today. If you want to talk about other things, I'd be happy to.

Oettinger: Let's stay with this for a moment because I'm sure there are a number of other things that the folks are loaded for since you opened up these matters. Security, in most discussions I've experienced, tends to be regarded as a kind of all-or-none thing. I mean, you're either secure or you're not secure, and the notion of degrees of risk and of what that means as a practical matter is something that I don't know how to approach. It seems to me that I would regard the studies that you described as something that's possibly doomed from the start unless that issue is addressed, because there's a price for the total slob and a price for total perfection and nothing in between. Nobody in his right mind would buy a fireproof safe, and again, the choice of words is deliberate, because that's been betrayed. Nobody who is not a shyster sells you a fireproof safe. You have a one-hour safe, or a two-hour safe, or a blazing-inferno safe, or whatever, and it's priced accordingly, and you expect that one of them will last until the firemen come. One will last even if it's in the middle of the Waco cult conflagration, and el cheapo will burn up if you don't put more water over it. Have you had a chance to run through or to conceptualize this question of, if you are buying, you pays for what you get. But what is it that you get in security?

Stewart: The whole philosophy of moving from what I call total risk avoidance to what we would call risk management is exactly what you're saying. The identification of the value of information that you are trying to protect has to come at the front end, not the back end. So there definitely will be an effort. We talked a little bit about reviewing our whole classification standards, but also identifying the value of the information to be protected and making some decisions from the managerial level about assuming zero risk or a little bit of risk or whatever.

Oettinger: That would run into people whose names I am trying desperately to recollect, but I can look it up, who were in the commercial business, trying to sell entertainment database type things, et cetera, but they explained they had algorithms that make it efficient essentially to encrypt things almost byte by byte, and when you put your money in the slot, they send you the key and whatever it is that you paid for gets decrypted, and they seem to have some way of ensuring that you can't then resell it without its evaporating or something. So, to the extent that these claims are even halfway reasonable, it sort of says that on information and inventions you ought to be able to lock it up totally tight and use it wide open if only you can figure what it is you want to do. Is that a reasonable view to take or am I getting sandbagged by somebody?

Stewart: You are talking about encryption things, right?

Oettinger: Yes, I'm talking essentially about selective protection of every piece, so almost every piece of it is able to be encrypted. You can sell it by the byte.

Stewart: One of the things that I think that we need to look at, aside from getting information to those that need it, is the availability of information, and we also have to think very seriously of ways to assure its confidentiality. Now, I wouldn't include the intelligence business in that, but this is a much broader kind of issue that we are talking about: information confidentiality, as you put it. I think that technology is moving by leaps and bounds to do that, but at the same time (and I am not going to pick on any particular agency here), I think for many here, when you talk about securing information, let's say, in computers and information systems, you have this very dynamic team of six white horses, which is the technology leading information, and then this awful-looking cart behind it trying to devise ways to protect the information. We definitely had to move from the philosophy of having a secure little box for this that doesn't match anything else.

Now that you have wide area networks and local area networks, you have to put more money into technology for information systems security and get it to the customer a whole lot faster than we ever did in the past. Customers aren't going to wait two or three years for us to certify, evaluate, and accredit an information system. By the time we get it all certified and evaluated and accredited, it's just old technology. So those are definitely considerations.

Student: I would like to do it in three years, but five or six years is probably more accurate in most cases.

Stewart: Yes, I believe that's true.

Oettinger: Want to move on?

Stewart: Yes. I wanted to talk a little bit about threat analysis and what we mean by threat analysis. I think, particularly in today's environment, that we have to get a lot smarter about doing threat analysis, and threat analysis in a broader sense, not just what the French intelligence service is going after — industrial secrets. I mean sophisticated threat analysis by which program managers and security officials can make some judgments about what risks can be taken. I think that it is a new way of going about a counterintelligence area so that we can get new ways of interacting, new ways of sharing information. We can't act any longer like separate fiefdoms in the counterintelligence business. We are going to have to learn how to share information, and the FBI is going to have to learn to share with the Defense Department and the Defense Department is going to have to learn to share with the CIA. We are going to have to move data through a common database in order to be able to make these judgments.

Oettinger: If you only knew the excuses made to me, that Hoover wouldn't talk to whoever was. . . . Hoover's been dead now for a long time, and this thing lives on and on. It's amazing! You know, it's this "déja vu all over again."

Student: Are you sure he's dead?

Oettinger: That's right, it's a conspiracy with Elvis. No doubt about that. But again I wonder whether you have any thoughts about why we have the perennial character of these things.

Stewart: I would simply say that it's a matter of turf and holding onto one's own perceived powers, and taking credit for things that are judged as successes.

Oettinger: Is there sort of an absolutely fundamental cultural problem there? It's curious, because if you look at people from slightly different cultures, let's say from a basic science culture, they've managed, by and large, to enforce sharing even though there's a great deal of turf with a great deal of variety on it and it's not easy because folks are convinced it's a whole fact. But, by and large, the culture is such that the price of not sharing is so high that you can sort of lose your professionalism. That doesn't mean that some folks don't occasionally do that, and if you read something like Watson's *The Double Helix* you get a wonderful sense of the imperatives that, even in the most open and sharing culture I know of, impel you to screw your neighbor rather than share. In a culture where the ethos is entirely different, where you've got all the compartmentation, et cetera, et cetera, so that you don't even have to worry, in a way maintaining it close to your chest is kind of the right thing to do, and it's not a surprise that it happens. But still the silence contradicts . . . does manage to enforce, it seems to me, sharing to a higher degree . . .

Student: . . . to a higher degree?

Oettinger: There's something fundamental about human nature that says, "I'm going to beggar my neighbor before I get beggared myself." Maybe one ought to accept that as a given and figure out how you live with it better rather than try to eliminate it. I'd love to foment some discussion on it, because to have a phenomenon deplored year after year and yet remain such a bedrock of the nature of the "career intelligence community" is a joke in one way if it weren't so serious because it is a masking, a block to efficiency and effectiveness.

Student: Are we just too blind, though, to recognize that for what it is? We want to attribute it to a problem with the intelligence community when, in fact, it's a problem with people and bureaucracies.

Oettinger: Yes, maybe, but if it is, then some combination of pride, cajolery, threat, and so on will be able to invent something to shift the incentives.

Stewart: I think that some of the new legislation that the Director of Central Intelligence was given as far as creating incentives and moving intelligence community personnel around may be of some use, because in the past there was no way to force greater sharing.

Oettinger: Creating sort of an intelligence "purple suiter?"

Stewart: I'm not going to sit here and say that centralization is the greatest thing in every single instance, but I will say that you can't make a cultural change — it doesn't matter whether it's in the CIA or anywhere else — unless you can change the incentive packages that go along with each individual's career path.

Student: It might also perhaps be, from my experience when I was working at the Embassy in Rome as the narcotics coordinator, that trying to get the different enforcement agencies to share information is almost impossible, even with an ambassador who threatened that if they would not, they would be put on the next plane, and he has actually done so. Remarkable! But nevertheless, I think there's much less risk in not sharing than there is in sharing and making a mistake in sharing it. That might perhaps be the reason. I don't know.

Oettinger: Let me ask you, Nina, about your last job in DOD. I'm not sure if it is just because I paid attention because you were in it, or I hadn't noticed it before, but is this the first time that these questions on counterintelligence were elevated to a high enough level so that one could begin to think about them? Or is there an even longer history of that?

Stewart: I think that in the counterintelligence business there's been a long history of people questioning the viability of the organization of the counterintelligence activities. I will also say that there has been some good progress, good movement, over the last two or three years, and it's structurally called the national agency structure for CI. There is a lot more working together of what I would call the CI operations chiefs. My task over in the Defense Department was simply to try not only to pool the counterintelligence apparatus, but also to make it relevant to the security programs. It was the first time, at least in my memory, that that was at least an objective of that position.

Oettinger: I hear that, but I also hear you commenting that essentially folks don't talk to each other any more than they did in the days of Hoover and so on. So I get the impression of something a little bit like one of these Escher staircases when the music in "Jeopardy" is on: it's always going up but it's still down at the same level. It's the illusion of progress but not really getting anywhere. If you look over 10 years of this seminar, I don't think there has been a session where somebody didn't say, "We have a problem with folks talking to one another but it's better. The green door is there but the TENCAP program will take care of it. It's better." And 10 years later, it's the same problem. Now, is this grousing that doesn't change, or is it the situation that doesn't change?

Stewart: I would say that this is part of human nature and that you're always going to have this problem to one degree or another, and where you sit is where your position is going to be most assured. I can't speak for 15 or 20 years ago because I wasn't in the business then. I can say that in some areas the information sharing does improve, but it only improves when we pay top-level attention to it. It may only improve for as long as they talk and low litigiousness is focused on it, and then it reverts to the same situation.

Student: Can the customers do anything to help this? After all, either at the executive or at the senior military level, the people who actually are the ones who get the information are the ones being screwed by the lack of communication at the lower levels. Is there anything that they can do about it?

Stewart: What I'm hoping for out of this whole effort is that the military services particularly will join in as customers to help us try to revamp policy and procedures, not just in DOD but across government. The more we solicit customer input, the better the product is going to be.

Oettinger: You shifted slightly, put one of the oldest problems in the intelligence business and you've had a chance to look at it from a number of perspectives and we're entering now a brand new one: "Oh, if only the boss would tell us what he wants," (the boss can be the President, he can be the agency head or someone elected and so on). Is that a solvable problem? It could even be the ultimate requirements.

Stewart: Let me put it to you this way: Jim Woolsey wants very much to solicit input from every layer that he can. Whether or not that's a realistic goal, I don't know.

Oettinger: Well, it may be a very realistic goal, let's say in terms of society and cosmetic relationships in keeping things happy. You have either required experience or not, in a sense that it contributes to setting requirements to steering analysis or the like.

Stewart: I think it does. Not in every instance, but I can think of several instances where some lone analyst raised an issue that no one else had thought about and it became . . .

Oettinger: Yes, but that's the analyst, that's not the customer.

Stewart: Right, but then that depends on how you define customer.

Oettinger: Okay, sorry. So to you the analyst is the customer of collection?

Stewart: Sure.

Oettinger: I was thinking of the policymaker. I'm sorry. Let's go back to where you were saying that Woolsey is seeking inputs. This is from policymakers or from the litigating community?

Stewart: It's obvious he's going to seek input from policymakers. He won't survive without that.

Oettinger: Well, but he also has a long history of being purely cosmetic. That's the problem.

Student: You're saying that the Director of Central Intelligence doesn't ask the President?

Oettinger: No, asking the President is a necessity, because otherwise you don't survive. Acting on that in a meaningful fashion, or presuming that the President — this President, any President — has the vaguest idea of what he or she wants, is a much larger assumption. It's again the history of information staff functions, whether it's at the corporate or at the national level: the perennial plaint of the professional is "My boss doesn't tell me what the requirements are." Professionals always say "If only he'd tell me, if only I could ask him, things would be better." Then some do ask, but they don't get much time.

Stewart: Having been on the side where there will be a principal's name, for example, and he comes back and says, "The President wants X, Y, or Z," or "It looks like we had intelligence gaps here," he's very alert to those kinds of issues and relays that concern immediately to those that can help fill the gap. So I guess it would depend on what you're talking about. My experience in his office anyway is that he's very much attuned to asking what's expected of him and . . .

Oettinger: But that amounts to deliberating — from assets in organizations to charts already in place.

Stewart: That's more difficult, right.

Oettinger: And that says nothing about the problem of what your planning is like and what it's like in terms of what changes you make by way of new assets.

Stewart: Part of the dilemma, particularly in the scientific and technology ends of the arena, is that by that time you're using investments that you made 12 or 15 years ago. It's not easy suddenly to turn that system around at the whim of a new requirement or a new need. That's very difficult to do in some cases. So maybe what he's seeing as a lack of responsiveness is simply because it's hard to do.

Oettinger: Shall we just move on?

Stewart: I raise these issues with you and these are really my personal views, and I'm interested in what you think about this whole area, not just CI and CM (countermeasures), but anything else if you want to discuss it.

Student: The tone I get from your remarks is that you side with the perception of being very reactionary . . .

Oettinger: Do you mean reactionary or reactive?

Student: Reactive, I'm sorry. Very passive, I mean, instead of having a plan. My question, I guess, is: what drives the intelligence community, is there a strategy, is there a game plan? You get a budget and you react to a budget. I couldn't get the answer that I was looking for. Randall Fort, when he was here six weeks ago, basically told me it's too hard. You want to fight everybody at once, so you end up fighting nobody. I'm just kind of curious. When you come up with a plan, where do you get your direction and how do you go about setting some type of focus for the whole intelligence community? Is this a set margin, or is this the direction we're going in, in the 1990s and on?

Stewart: Let's take the budget as an example. I think that the way the budget was formulated in the past has not allowed for cross-program evaluation and hasn't been flexible enough to allow for changing requirements in a changing world. Instead, once something has become baseline, then it's there forever. I think I can tell you beyond a doubt that my boss has issued instructions about how to make the budget process responsive to the changing environment. You have a national security strategy (granted that strategy may change with each President and in fact does), but if we aren't able to adjust the intelligence collection and production efforts to meet that strategy, then we deserve to be slashed. So I think that you are about half right, in the sense that it has been sort of a machine that people have found

too hard to manage or found too hard to get their hands around because it's not lent itself to evaluating air breathers with satellites, with HUMINT collection. It didn't lend itself to that kind of analysis. That's got to change.

Student: Yes, I can imagine it's a huge problem. I was thinking exactly along the same lines that you are, that there is a national security strategy and correspondingly there is a national military strategy, and I know the intelligence side is a lot more secretive. There must be something in writing. There must be some type of direction. It's just that at least the public doesn't see it very often. It doesn't see any type of concrete goals, and maybe that's part of the problem.

Stewart: Yes, that's true. The budget is not something that is debated publicly, and neither is the amount of assets that one spends in a particular area.

Oettinger: Yes, but I think maybe it's no longer so, if it ever was! I had a good friend who was a high official on the National Security Council staff. Now is not the time to tell you the story he told me over a beer in full gory detail, but it essentially encompassed a career looking for where the decisions are made and where the guidance comes from, and at each stage being told that it comes from the next layer, until he found himself on the White House staff and found that he was it and he hadn't the vaguest idea. There was no place left to go, whereupon he left government service and went back to the private sector.

I think the notion that you can look for "them" and find "them" is more often wrong than right in the United States of America. There may occasionally be some guidance document, but by its very nature it's likely to be the product of decisions and thought processes, perhaps from the last administration, or by folks who are thinking while they were out and haven't had time yet to revise what they thought when they were in the private sector or academe or whatever, and now they've got the responsibility they may think somewhat differently. So, it seems a little bit at odds with your response, but sort of lets you comment on it. It might have been more often than not that "they" do not exist and that the implications of "them" not existing and therefore making it the responsibility of a staff, let's say an intelligence staff or a logistics staff or whatever, to think for the principal. I'd like your comment on that.

Stewart: Each administration has its own way of setting policy and making decisions. Whether it's called a principal's meeting, or a deputy's meeting, or a PVD, or PRD, or whatever, there are decision documents on a whole range of foreign policy and national security issues that are supposed to guide the government in how it does its business. Each administration fools with that a little bit, calls it something different, reviews the past administration's decision documents and either validates them or invalidates them and issues something new. But those are things that the administration knows that it wants to pursue, where it knows that it has a particular goal in a certain area. But his point about surprises and the need to inform when things change in country X has not been part of the policy decision process. This is a decision that is something the intelligence community has to do. Its warning function, to me, is its most important function.

Oettinger: It seems to me on that comparison issue, that is something that you cannot prolong.

Stewart: Right.

Student: But your collection responsibility is what the DCI and the President and the State Department formulate as the intelligence community's collection priorities. The Soviet Union fell off the face of the maps, so the priorities went way down. So then you take your resources and you have to respond. Those programs have to respond to the Director or to the President in how they are reacting to that.

Oettinger: Yes, and this is another deep organizational dilemma, which is why you are reading about folks who have been dissidents in their own organization, et cetera. If every organization were to follow the exact program, the odds of error would grow enormously, so that creative insubordination repeatedly has an important role to play, and if it goes too far, of course, you have chaos and anarchy. It seems to me that in every organization, I want to add that to the list of tensions and balances here, because if you follow that recipe, then you get a bunch of sycophants, to be polite about it — bureaucrats who follow orders — and that gets very difficult. Yet the other extreme is anarchy, and I can find that in the intelligence community. There has been enough latitude before, or enough anarchy, that things have never gone seriously wrong; there's nothing too bad. But, to me, it is one of the most serious organizational dilemmas, especially in institutions that have the secrecy and compartmentation. They do play a role both ways normally because you can't have some comfort of one sort or another unless they manage again by bureaucratic stultification to kill any of that off. The black

programs may be the last refuge of an occasional thing that isn't completely cut-and-dried with past history.

Of all the tensions or balances that we talked about this semester, this is one of the most critical, because it impinges on everybody's personal decisions and career. When do you follow the party lines, the policy, whatever you want to call it, and when do you apply your own judgment and say that "they" haven't thought of that, and I am "them" and I am going to risk court-martial, dismissal, or loss of clearance, or whatever because I think it's right. Most of the time it isn't quite that dramatic. You have a boss who puts something in the budget and quietly gets things started. The only reason IBM survived this far as an institution is that they've become masters at doing that.

Student: I have a quick question regarding information that's in the system. I'd take terrorist organizations as a good example of a target that we will always have. Within the military, for example, attachés are routinely assassinated. We've had them assassinated in Greece and on a couple of occasions in the Philippines. They've been targeted on a regular basis and postmortems or investigations that are done afterwards tend to reveal (at least I've heard this anecdotally) that information that could have prevented the attack was available in the system but didn't get to the people who needed to use it. From your experience, from your perspective at OSD, what postmortems have you seen that reveal that type of problem and what did we learn from it? What action was taken to try to rectify or change the system?

Stewart: As we talked about, one of the initiatives that we had pursued with some success is still not on line yet, but it was the common CI database. There was an awful lot of resistance to having this database. It's based, by the way, on the same sort of terrorism system. But there was some more resistance again because each organization was concerned about who was going to get access to his information. Even though they didn't have any information systems to begin with, there was a resistance to us doing this.

Oettinger: You're saying that the resistance is because they don't have something and they're ashamed to admit it?

Stewart: Oh, yes. But I would say that the inability to move information, particularly among the investigative agencies, to me is the single greatest impediment.

Oettinger: Unfortunately we're running behind in the publication of proceedings, but last year Al Lubarsky, who was the counternarcotics man in the Office of the Secretary of Defense and still is, detailed some of what Nina was talking about right now. If it's important to somebody's paper, I'll give you access to the tape. You can listen to it in the office. There's more to come. Bringing all that stuff together is a Herculean task.

Student: You mentioned the CI database at lunchtime, and the reason I was intrigued about that is because I know from the work I did that different agencies have different message formats that are not compatible. They also have different policies and protocols that don't interoperate. How bad is that?

Stewart: But that's just a software issue.

Oettinger: Well, it's a software issue, which is often used as a smoke screen for the turf issues that we have discussed. I will make a flat-out statement. There is in 1993 absolutely no legitimate, technical excuse for that, the way there might have been barely 35 or 40 years ago, but technology has done away with that. It's sheer obfuscation.

Student: But it happens.

Stewart: But it's the principle of the thing.

Student: You can solve the problem. It's empirical. But it's easier said than done.

Oettinger: But it should not be accepted as a legitimate excuse. It may be hard to overcome.

Student: I hate to agree with the Doctor on this, but he's right.

Student: I think another problem is not just that people don't sign on to the software or the message formats or the protocols that are necessary to create a consolidated common database or system where people can share information, but part of it is training. I know that in the Navy, civilian counterintelligence agents hate to write IIRs because they just don't know how to do it. They weren't trained to do it.

Student: Lack of initiative?

Student: It's also lack of initiative, and the only ones who ever did it were people who had military experience, who had worked for CTF168 (Combined Task Force), for example. They had cross-pollination and understood how to write in that message format. Otherwise, NIS (Naval Intelligence Service) agents would opt for the easiest solution,

which was to write what they called a NORP, a Naval Operational Response Plan text, pretext. The problem with that was there was no way to put that into a database. Unless it fell into the hands of the right analyst, which usually it would not, because there was no lateral system for dissemination of that kind of information to the other people who could use it, the information was in the system but unavailable to the people who might be able to use it. That's an institutional problem. It's a training problem.

It's a problem with mindset also. For example, I know that investigative agencies view a terrorist attack where there is loss of life as a homicide. It becomes an ongoing investigation, and they're loath to share information with anybody else regarding what they're finding out during the course of what ends up being an open case in perpetuity. They almost never solve those, and so the information is stuck in the system and unavailable to other agencies that might be able to use it unless you actually bash in the door and make a really strong case for why you need it. It doesn't flow freely, and I see those as impediments in the system.

Stewart: The CI side of the house doesn't do a lot of intelligence reports. Here's another instance with military services. Up until last year they didn't track deserters who held sensitive positions and we had a case or had a conviction on a fellow whom we should have picked up probably six or seven years ago. Neither did they talk to one another about him, but they also didn't keep records in the CI side. They didn't follow the deserter case in terms of the sensitivity of his position. They just had him labeled as a deserter.

Student: You were talking about career paths earlier, and I've spoken with people like Dusty, Jim Worthington, who is with the Agency, about how the CIA, for example, brings in new blood, or how they bring in people with special skills that they might need, maybe an international banker or an accountant. At least a couple of people whom I've spoken to have said that bureaucratically there is no way to do that very easily, and lateral accession into the agency or other intelligence agencies is actually rare.

Stewart: You mean lateral level, or entry level, or high senior level?

Student: Yes. And people who might be interested in working in the government in the intelligence field are discouraged from doing it because they have to come in at the entry level.

Stewart: Well, it depends on what you're talking about. If you're talking about the NIC, the National Intelligence Council, that's not true in that senior academics and people in the private sector are brought in as senior folks to work in the NIC. That's different. It really depends upon which directorate you're talking about and what positions you're talking about. If you're talking about someone coming into the Directorate of Operations who is a mid-level case officer, then you're right, that doesn't happen very often. I can't say as much in the DI (Directorate of Intelligence) but there may be a little more flexibility in DS&T (Directorate of Science and Technology).

Student: Do you think there needs to be more lateral movement of skills and unique backgrounds into another intelligence community?

Stewart: There definitely needs to be, particularly in the areas of science. They have to have qualified people, specialists, who are bright and talented continually coming in, because that's something that needs a constant flow, and you can get stale really quickly in that business. I think that in the current downsizing environment in the intelligence community, the CIA in general, that our challenge now is making sure there is enough headroom and that there is an inflow of new people, small as it might be, while we keep treading this downward slope. That's going to be very difficult, and whether or not that also gives a lot of room to mid-level sorts of transfers, I don't know. You can't do everything. That's the problem.

Oettinger: But I think what you're addressing is something that is not peculiar to the intelligence community. It's again a balance, tension. Any organization that does not renew itself with outsiders is going to be dead and buried very quickly. Any organization that just fills itself with outsiders will have no tradition, no competency, no esprit de corps, no common understanding — the primal understanding that means that when you've got a strange situation you can count on your neighbors to react appropriately. So that is on that long list of things that I hope you've been compiling here this semester of unanswerable questions that you may at any given time be expected to answer. It's always a matter of adjustment, because either extreme is absolutely untenable. That's about the only safe assertion you can make. You cannot run an organization that is at either extreme, and once you're in the middle, you're going to have to make decisions based on this particular situation, particular budget,

particular world, et cetera, et cetera. You tweak it this way or that way and that may even depend on area by area. This year will be different from next year.

Stewart: Along with that comes the constant need to train and retrain people, and unfortunately one of the first things that usually bites the bullet in a downsizing environment is training and education, and it ought not be.

Student: You hear a lot of talk, and it sounds like a real bureaucratic nightmare in Washington. Can you tell me about some of the positive aspects of being in the intelligence community and professional fulfillment? It's just that it doesn't sound attractive with all of the things you hear about it. Just what are some of the motivations that people have for participating and what are the excitements? There must be something.

Stewart: Let me start off by saying that a lot of you in here have an intelligence background or are in the intelligence business. So, when we were talking, you tend to talk about the things that grieve you more than things that don't. So let me start out by saying that the things that we talked about today are things you probably find in any major corporation or anywhere else in government. Probably any employer would have some of the same sorts of problems.

The thing that attracts one to the intelligence community, and I'm just speaking for myself now, is that we have an opportunity to make a difference. You have an opportunity to become involved in the innermost workings of government and its national security and what's important to the government, and you do have the ability to make a difference. It's exciting and it's challenging. There are very qualified people who have tremendous capabilities who tend to come to the intelligence community. So there is a camaraderie there, and there's opportunity and there's a feeling that you can make a difference. That's my rationale.

Oettinger: Yes, that pretty much makes sense, since you implied that is an atmosphere that I create. I would answer simply, similarly to Nina, that one tends to look at the worst and draw attention to how you survive in such environments and make them function. I share Nina's enthusiasm and her assessment of the reasons why one works in intelligence. One of the reasons why bureaucracies in fact do work is that they have a sufficient number of intelligent, dedicated people who do not necessarily take literally all of the injunctions of the bureaucratic system. It always amazes me that the system works. I think that is because the air traffic controllers do not follow the book literally every day. When they do, you know what happens to you in an airport, and fortunately they strike a balance between familiar airplanes to track and following literally what it says. Also, we travel successfully because there is one segment of the bureaucracy that manages to strike an appropriate balance for itself. I just happen to have this belief that if you understand what you are balancing and what your trade-offs are and what the structure of the bureaucracy is, you have a better sense of what you need to do, want to do, and are able to get away with, and you need to get away with it.

Stewart: Did any of you ever read the famous James Wilson book on bureaucracy?

Oettinger: That's a good one. He is a former Harvard professor.

Student: Is that good or bad?

Oettinger: Then he went back to California.

Stewart: He went back to California, but he was on the President's Foreign Intelligence Advisory Board and so I had the pleasure of working with him on a number of these intractable questions dealing with the intelligence community. I would just recommend that you read it, because it crosses both the government sector and private sector. It kind of puts a humorous twist on it, but at least it was a little bit of realism about it as well, and this kind of self-reflection is actually healthy.

Oettinger: Thank you. I should add the book to the bibliography. It is not on there now, and that is an excellent suggestion. It's James Q. Wilson's *On Bureaucracy*. There is still time to do a critique of it, but I would hope that by now you find this reading worthwhile for fun and edification as well. That is, it's a good book.

Student: Has there been a change in attitude about intelligence given the change in administration from the Bush years to the Clinton years, and, if so, what kind of change in attitude has the administration had?

Stewart: Change in attitude to what?

Student: Just in a general sense of its importance, its usefulness, its reliability, and any of those kinds of issues.

Stewart: About the intelligence community?

Student: Yes. The senior policymakers.

Stewart: Yes. There always is, at least in the positions I have held. I have noticed a difference in each administration's attitude among the senior brains, and a lot of it is personality driven, but some of it is just simply the priorities of the administration. For example, George Bush was an intelligence junkie, having been the DCI, and he loved it. There was constant to-ing and fro-ing with the intelligence community because George Bush really liked to hear it. He made time for it on his schedule. Some Presidents haven't. Ronald Reagan particularly liked listening to some of the stories, but he was not as approachable from the intelligence end. Some of his questions were very keenly intelligent. He liked to enter into give-and-take with what he was hearing. He questioned deeply. So depending on whom they surround themselves with, there is a different attitude from time to time. Some are more approachable than others. But it is personality driven.

Oettinger: That is interesting. There is enough on Franklin D. Roosevelt written in terms of his active manipulation of surrounding staffs that he created and he was usually effective. There is more and more coming out on Eisenhower. During the Eisenhower years, one got the impression of a rather stodgy President who hardly could pronounce "nuclear," and his love and understanding of intelligence and the extent to which he essentially created much of what is the intelligence community today are vastly underrated. It is awfully hard to close in without having some of Nina's essential direct experience. The histories don't catch up with this stuff very quickly, but you can get a pretty good picture by now, let's say, of FDR, Truman, and Eisenhower, and the styles couldn't be more different in terms of what they did with the formal intelligence establishment. Roosevelt simply did not use the stuff. Eisenhower essentially created the formal apparatus that we have today — that gave it its structure. So, if you go a little bit further back, you can take what Nina said and completely agree with it. There is a good deal of unclassified detail in the biographies of the Roosevelt, Truman, and Eisenhower administrations. It's beginning to come out on the Kennedy years, but there it is still a little bit squishy. And beyond that it is still classified.

Stewart: George Bush used to make a point of going to the different agencies, and that was rather unusual. He visited different agencies at different times in his administration. It seemed to me to raise morale at those agencies when you had the President show up for an event.

Student: His departure speech was very moving, especially in terms of boosting morale.

Stewart: Right.

Oettinger: Over lunch, I mentioned to you the book you talked about a little bit, which is your interpretation of this call for greater reliance on open sources and what that means and what its implications are.

Stewart: I think that it is a misunderstanding if one believes that in the last 30 or 40 years the intelligence community has not been an open source of information, because open source information has been a part of its business all along, particularly the analytic products. I think that this big call for using more of the resources is simply because there is more open information out there because of the information revolution, and so is the call relative to more integration of open source information with intelligence.

I think you are right, Tony, that the intelligence business exists to find out secrets and report secrets and that you can't lose sight of that. But I'm saying, as a token, if that were all they did, and it wasn't related somehow to the open literature, I am not sure that it would be all that useful.

Oettinger: With that particular set of issues in mind, it seems almost contradictory to tighten the budgets because it seems to me that if there is one place where in a tight budget area and situation, you would say, I want to do less of the stuff that others can do. So I'm asking the question in a spirit of how one reconciles that so that you get maximum from the intelligence community along lines that cannot be done elsewhere, without sacrificing the quality of intelligence. It is clearly again at one extreme if all the intelligence community ever dealt with was what it collects and never put it in the context of anything else. You'd get one hell of a weirdly distorted world view. On the other hand, if everybody at any intelligence agency, in any part of it — military or civilian — were simply to do what a dozen open sources do, you don't need an intelligence community because you can call at Harvard University. So I guess I'm pleading for any thoughts you may have as to where you draw the line.

Stewart: I think he draws the line on a budgetary standpoint. If a new open source initiative is one that is going to cost $5 billion to translate little-known documents in Byelorussia, you're not going to do it. But if you are talking about upgrading your information systems to include open sources along with everything else so that you have a better communication flow, then it is a different subject. So to me it is a matter of cost-benefit trade-offs and using some rational system. But I think that calls for open source information get a little bit confusing, at least in some of the things that I have read about doing a better job on information handling.

Oettinger: Meaning what, precisely?

Stewart: Meaning that in some areas of the intelligence community information systems are not capable of handling large amounts of data and helping an analyst, for example, given the wider range of choices by which to complete his product.

Oettinger: Is that synonymous . . . ?

Stewart: I don't think they ought to be competing.

Oettinger: Yes, or with LEXIS and the others. Where do things stand on the question of folks going back to tie that threat in with security, then? Is it a matter of an analyst having wires and mail pouches going everywhere in front of him, or her? If you pursue that information management thing, then you get into questions of diverse sources converging into one location, and that on the whole has been kind of an anathema over the years.

Stewart: One of the things that the Director has been pushing very hard, and with a lot of success, is to generate more products on a quicker basis, and fewer products like these long-range analytic tomes that are scheduled to be completed in 11 months and then you come out with something unbelievably thick. So there is a lot more emphasis on quick and dirty sorts of things, analytic products that are relevant right now and that are completed in a maximum two weeks' time frame.

Oettinger: Again, that leads me to an interjection which several of you may have made in several of your latest draft papers, because that problem also has a long history. What you are telling me is that the balance is shifting toward the shorter term. If it shifts that way long enough, somebody will reinvent Sherman Kent's *Strategic Intelligence*, and a number of you who have not read Sherman Kent's book, which is now almost 50 years old, would find it well worth reading, because Sherman Kent came into the OSS (Office of Strategic Services), not the CIA, essentially in a situation where everybody was oriented to short-term stuff — next week, or whenever it was needed for the next military operation in World War II. His point was that a national intelligence system that did not take a longer-range view would just condemn one to react to yesterday's news. There is a long history of that which may, in fact, be coming to an end if Woolsey has his way and things get cut way back to short-term things.

Stewart: Not everything.

Oettinger: I understand, but that is another one of those critical elements for which there is no answer.

Student: Is the pressure on short-term intelligence now with the situation you're describing because we don't have any long-term framework for things? Is that it?

Stewart: No, and please don't misunderstand me. I am not saying that long-range analysis is not good and is being done away with; quite the contrary. It is simply that the time it took for an analyst to write a product and then get it vetted, the management layers that that analyst went through in order to clear a product, have become so unwieldy that he would have to stop off at 12 or 15 places before he could get an item published. That is simply not acceptable. Its quality control is great, but when you get to the point where you are putting in three and four additional months just to get a paper published because it has to go through all these hoops, then you are really not trusting your analyst to write a quality product in the first place.

Student: So what you are saying is it is not so much the goals that they are looking at, it is just how long it takes to do these things?

Stewart: Right. The management layers for reviewing these analytic products were just incredible.

Oettinger: I'm conscious that we only have about eight more minutes, so let me urge you to speak about whatever is on your mind, or was when you came in, or that we should have asked and haven't, and you are wondering why we didn't. Please.

Stewart: Well, I hope you pursue a lot of your questions. I hope you keep after it, because we constantly need an interaction and exchange from those of you who are looking at it and who have the time to look at it and say, "Well, this isn't right," or "Why do you do it this way?" Part of the problem

with any management structure at our level, or anywhere else, is that you tend to get your day filled for you for a long way out, and consequently what I hate the most is that I have lost the ability to sit back and think about things the way that I could when I was over at the Intelligence Corps. You could sit back and think about something in a more leisurely, long-range fashion, and sometimes we get caught up from our level with putting out the fires of the day. So, I think it is important for you to continue these kinds of forums. I think they are good, because they force the system to think about things that might not come to our attention. I would also encourage you to continue to push that through your own studies, through your own questions. Do you have a response?

Oettinger: This is very important. Let me extrapolate because I think most organizations, and that's universities, private sector, anyplace in the government, tend to run on what folks thought about, and so the notion that you'll do the thinking when you have to is not quite right. There are some who could appreciate those comments. Anything else?

Student: One issue I hear a lot about is that we've got a lot of material and we're putting it together, and we're collecting a lot more than we can analyze and digest. Part of that digestion factor comes in with the decision makers and policymakers who are using intelligence, and in many cases that I've investigated, I found that it's not that the intelligence doesn't exist, or that it didn't get disseminated, it's just that it didn't have the right kind of priority placed on it by the decision maker. It wasn't used, perhaps, the way it should be. What can we, within the intelligence community, do to facilitate teaching our decision makers how to use the intelligence?

Stewart: I'd have to have some specific examples that you have in mind. Let me put it to you this way. If something is buried on page 15 of the NED and it's only a bullet, who's to blame?

Student: Yes, precisely. Let's say you've got a general officer, and he thinks that a huge study that you've done on a certain event or weapons, which is four years old, and the doctrine of the target country hasn't changed in 40 years, [needs to be redone?] and you've got more important things to do like the acquisition of modern weapons systems from an allied nation. How do you go about trying to tell these people that we can use this type of intelligence if we can forget about marshaling the resources against this aspect? Does that just come down to the old bureaucratic person-to-person type of thing, or do we have some way of showing these guys?

Stewart: One of the things that the intelligence community can do better in order to forestall those kinds of problems, and we need to do more of that, is briefing senior officials as they come on board about what intelligence can or cannot do for them. We have such a constant changeover in the senior administration ranks that we sort of lose sight of that and then we wonder why it is that the general officer here, or this assistant secretary there, hasn't used what we've given him or is asking some silly questions. I think we need to brief our capabilities better than we do. We tend to be insular, not necessarily because we're trying to hide anything, but because that's sort of the way we are. It's a tradition and we don't tend to reach out and say, "Here's what you ought to be thinking about."

Student: Do you think we're doing a good job, given the mixture? When you had somebody like Bush, who used to be DCI, it's a lot different than when you have somebody coming from Arkansas. Are we doing our job?

Stewart: Yes, I think so. I can point to several different individuals who may not have received as much of a briefing as they need, but then I'll look at others and I would say that they're using the intelligence very, very efficiently. So I think we're doing a better job of it, but it's not systematic. We probably ought to get more systematic about it.

Oettinger: Okay, the time has come for us to thank you and I do. We've got to get you to the airport.

Student: And we've got one quick thing, if somebody could hand me that.

Oettinger: Oh yes, a small token of our appreciation. Now the couth thing to do would be to open it so you could look at it and so on, but it's wrapped so nicely to get back on the airplane with you. I will just tell you that it is a picture of a Harvard landmark, which we hope you'll enjoy as a memento of having been here.

Stewart: Thank you very much. That's nice. I've enjoyed it. Good luck to everyone, and I hope I get to talk with some of you again in the future.

Oettinger: Thank you very, very much.

INCSEMINARS1993

ISBN-1-879716-12-7