INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

The Role of the National Security Agency in Command, Control, and Communications
Harold Daniels

Guest Presentations, Spring 1986
Clarence E. McKnight, Jr.; Robert Conley; Lionel Olmer; Harold Daniels; Mark Lowenthal; Richard J. Levine; John Grimes; Bobby R. Inman

February 1987

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.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
I-87-1

The Role of the National Security Agency in Command, Control, and Communications

Harold Daniels

Mr. Daniels became Deputy Director for Information Security of the National Security Agency (NSA) on January 1, 1986, following three years as the Agency's Assistant Deputy Director for Communications Security. He entered cryptologic service in 1954 as a Navy communications technician serving at NSA, and joined the NSA staff in 1957. Since then, he has held senior management positions in both SIGINT and COMSEC disciplines, including assignments as Director of Civilian Personnel, and Chief, Asia and Pacific Analysis Group.

I appreciate the opportunity to be up here this afternoon and to talk to you a little bit about the role of the National Security Agency (NSA) in the command, control, and communications business. It is basically one of providing the systems that will give security to the information that is held both in government and in the private sector.

I understand that some of your interest lies in the various information technologies and command and control vulnerabilities affecting multinational corporations and intelligence in the business world. I'm going to try and hit those areas as I go along this afternoon, but I thought I'd first give you an appreciation of the perspective from which we look at the information security problem in NSA. I'll be talking first about the telecommunications "explosion"; what we see as the threat to your information from outside factors, and sometimes inside factors; a little bit about the nature of cryptography, since that might be new to many of you; some recent government actions, which I will spend a lot of time on, especially the National Security Decision Directive (NSDD) 145 signed by President Reagan a couple of years ago; and then just a few of my own perspectives on information in the private sector.

There are many ways to describe the telecommunications explosion, but I think one of the basic words is change. Telecommunications is in an era of constant change, and of phenomenally rapid growth. New technologies are driving both the change and the growth. Technology is turning over in about every five years, and sometimes in even less than that. Finally, the merging of computers and telecommunications technologies is driving this explosion to replace many of the ways we had stored and communicated information previously.

I read that the first full-time radio announcer died this past weekend; he was at station KDKA. That's kind of where we all started. Since then, our communications technologies have grown and changed tremendously. Everywhere you look there is growth in the system. The computer industry is growing at the rate, I understand, of 12 to 18 percent a year. Telecommunications is also in rapid growth. Of course, the electronics industry that backs all that up is also seeing a growth rate of about the same level as computers and communications.

Not too long ago, cellular radio was something that was described in books. It was kind of a theoretical thing. Today, more than 60 cities have cellular radio systems, and you can get one from as low as $15 a month, depending upon what kind of service you have, on up to a couple of hundred dollars. The point is that it's growing at a phenomenal rate. Interestingly enough, some people seem to think that because you are now able to talk to someone from

your car, that information is secured from other people. There's even an ad on TV where a salesman is driving home, and he's a little late for dinner, but he has made what he thinks is a fairly good deal and he wants to get a bottom line price. He calls his boss on his cellular radio and he says, "Hey, how about this deal. I'm going to let it go for this. Will you go along with that?" The boss says, "Yeah." What he doesn't understand is anybody in that area, for a couple of thousand dollars, can get all of that information very easily. You've seen that even the satellite movies and Home Box Office (HBO) are now going to start scrambling their signals, because a person goes out and buys a little small dish and is able to get for free the HBO that you're paying for on your cable.

The point is that these new technologies are really driving the industry. People are communicating now who probably don't even need cellular radios, but they have them because they're there, and they use them because they have them. They talk about all kinds of things on them. I personally wouldn't want one; when I get in my car I like to be left alone. But that seems to be the way things are going.

Another thing driving the growth is that computers and communications are hooking up. You're seeing people with personal computers (PCs) in their home. They started off using them for games, then moved on to doing their income tax on them, and they've logged on all of their private financial information. Now they're beginning to use them for electronic mail through TELENET and a couple of other commercial systems. They go on the bulletin boards and pick up all kinds of information, and communicate all around. You're going to be able, fairly soon, to do your shopping from the local supermarket while you're sitting home at your computer. That's all coming. It's not coming as fast as some people thought it would come, but it's moving very dramatically, and especially in the business world. People are seeing that if they have their corporate headquarters on the West Coast and elements of their corporation on the East Coast and in the South, they no longer have to send, via air mail or regular mail, stacks of documents that cost a lot of money, as General Donahue pointed out this morning.* Rather, they're able to communicate back and forth through the local telephone network from their computer and pass all this information around and use it immediately.

All of this is possible because computers became accessible to the individual user. The ENIAC (for Electronic Numerical Integrator And Computer) was one of the first computers; it took up a whole room. Now, it's probably a mini. Everything it could do could probably be done in a small microprocessor.

Now, what's the threat? The major threat is that anything that goes out into the ether can be intercepted if you have the proper equipment to do it. There was a time when people thought that was a major job. It turns out that if you go down to the local Radio Shack and you're really interested in collecting someone else's data, you can build yourself a system to do that for less than $2,000. If you look at the roof of the Soviet Embassy on Sixteenth Street in Washington, you'll see that those antennae certainly aren't all for TV. The Rockefeller Report* that came out in 1975 explained what this threat was. You've read in the papers in the last few days that we're asking a number of the Soviet United Nations people, who are thought to be KGB types, to be sent out of the country. Certainly the threat from outside is present and active.

It's not only the Soviets who pose this threat; it's anyone who wants to invest in, or who already has, this capacity. The threat is a real thing, and it's not understood well by all. I can't get into too much detail. Let me just say that it's not a hard job for someone to find out about what you're doing when you're communicating out through the ether. It's not well understood by industry, and only, I would say, in the last five or six years has it really been understood within government — and even if understood, in some cases, not acted upon.

There are three important components to any decision involving information security: value, vulnerability, and threat. When one considers protecting information, one first looks at the value of it, then what the vulnerability is, and then what the threat is. If you have any combination of those parts, you'll probably want to do something to protect that information while it traverses the telephone system or whatever takes it out into the ether. The value is your own determination. You have to decide that. If

*Major General Robert J. Donahue, USA, Deputy Assistant Chief of Staff for Information Management.

*Report to the President by the Commission on CIA Activities Within the United States, 1975. U.S. Government Printing Office.

you value your information, chances are, someone else will value it. What vulnerabilities do you have? Well, if you're on a piece of wire between this room and that room over there, and you have some sort of protection around the enclave, chances are the vulnerability may be very small. If you're talking to the West Coast, that information leaves this building, goes perhaps on a cable to some microwave point, goes across the country partly by microwave, partly over satellite, and then goes back down again. Then that information, while it's out there on microwave or on the satellite, is vulnerable.

If you decide you have highly valuable information that you've determined to be somewhat vulnerable, then you have to say all right, now what's the real threat? If you're going to invest in protecting this, you've got to have some idea that somebody else has (a) the desire, and (b) the capability to take advantage of your vulnerabilities. That decision involves information that you, as an individual, cannot always have. It's my job, along with some of our other intelligence agencies, to help the government make that decision as to what that threat is. Under NSDD 145 we've also been asked to advise the private sector. We do that in such a way that we're able to explain to them what possible threats there might be to their particular communications.

Take the computer world, for example. There is a perfectly legal way that an adversary, let's take the Soviets for example, can get into a U.S. data base containing a lot of technology simply by subscribing to a public system (figure 1). For example, they can come in through Vienna into Dialog, which is a service offered by Lockheed, and get into the National Technical Information Service (NTIS) where the U.S. files on a number of projects and information and weapons systems are held. This is a clearly legal method for someone to get into that. Anyone is capable of buying into that system and getting that information.

What's our job? Our job is to make people aware that there is a problem out there, and then to do something about it. We're basically in the business of providing the technical solution to that problem. We're able to provide communications security (COMSEC) types of solutions, and we're working our way toward getting computer security (COMPUSEC) solutions to the systems in terms of a trusted system within the computer. That's kind of hard to do. There is a great big difference between communications security and computer security. We've been in the COMSEC business for 30 or 40 years; there is a mature technology that one can transfer into industry to end up with technical solutions. In the computer security world that's not the case. It's a new industry; the technology is not mature. It is extremely difficult to take in-place systems and add on to them to gain your security. We're going to have to look toward doing some of that to gain some degree of short-term security, while trying to mature the technology in partnership with industry to provide the long-term solution.

I thought I'd just spend a couple of minutes on cryptography. Cryptography is sometimes called "hidden writing." Back in the days of the Roman gladiators, it was an individual type of enterprise: The guy who invented the cryptology was the one who put it into effect. There was no such central organization as the NSA to do that. The way they used to send messages around in those days was to take a Roman soldier and shave his head and write the message on his bald head, let the hair grow out, and then send him off to where he was going. He'd get his head shaved when he arrived, and the message would be there. The problem was that you then had to get rid of the message, so you got rid of the messenger as well. That was the first one-time pad. The technique has matured over time. It worked its way into a number of paper systems, first electromechanical, and then, since World War II, into the electronic digital key generator, which is the way information is protected today. Unfortunately, there is still an awful lot of paper out there.

In fact, the NSA has the second largest printing plant in the world. We're second to the Government Printing Office in terms of output and production. One of my goals is to reduce that by a considerable amount over time. The amount of paper that's moved around is just tons, and General Donahue can tell you some of the problems with moving that stuff, and having it at the right place at the right time for the right person to use. It's a very difficult situation. It becomes even more difficult for the Navy where they have to be prepared to function in a number of operational areas. If you're out in the South Pacific and they chop you over to the Indian Ocean, you have to have with you the keying material that you can use to talk with people who are normally in the Indian Ocean. There's a lot of material that has to be carried onboard that ship, some of which is never used. If you never get chopped, you never use it. But you keep getting resupplied all the time. The

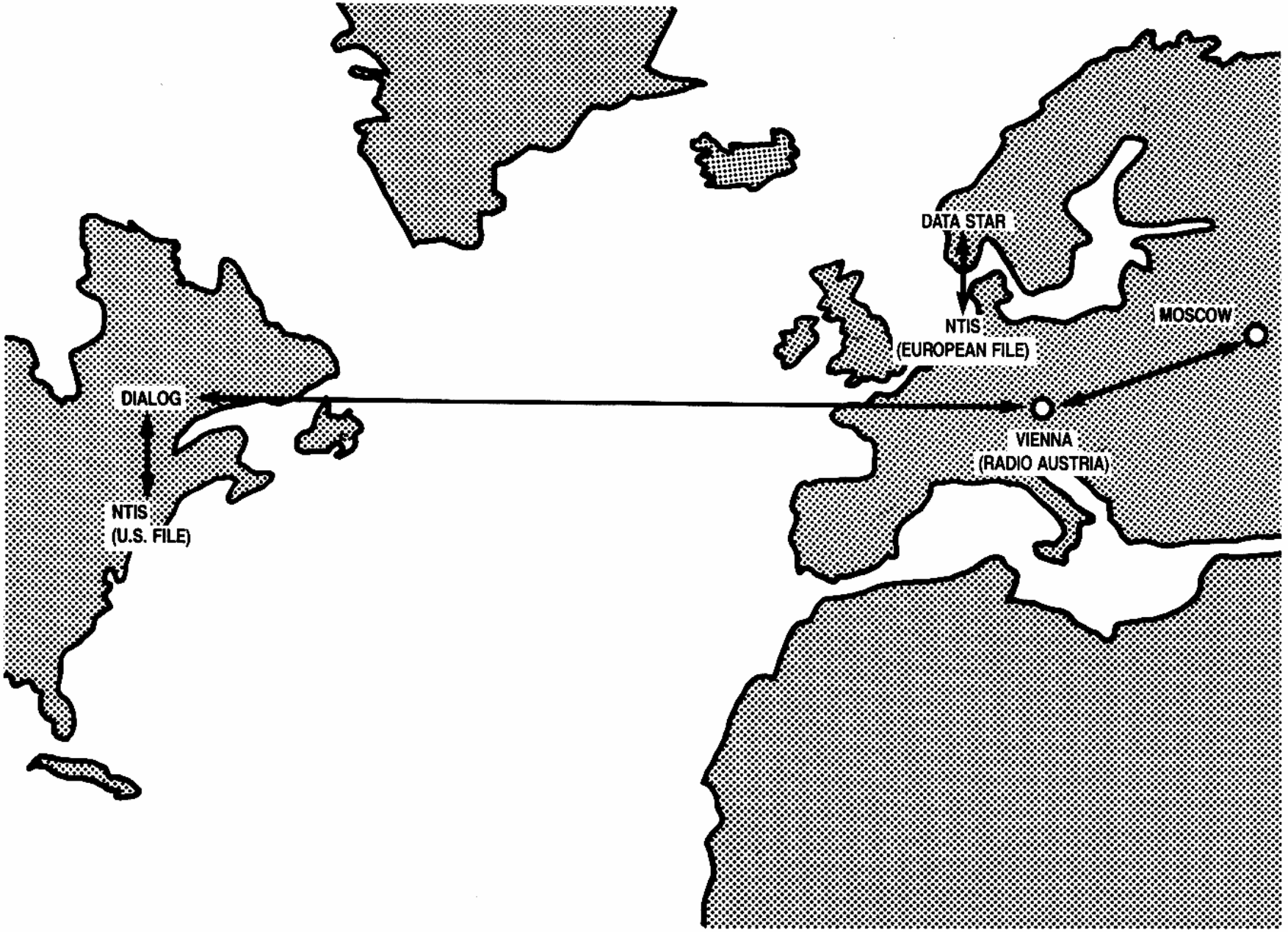

Figure 1. Soviet Access to Allied Data

solution to that problem is going to be our ability to provide electronic rekeying.

What do I mean by all that? The new general-purpose digital key generators that provide a trunk encryption take plain text, like what I'm saying right now, and put a random key against it to produce cipher text (figure 2). The fellow on the other end has to have the same key as you who are sending it; otherwise it would still be cipher text to him. That's why it's so important, and, as General Donahue described in the case of Grenada this morning, you have to have that same keying material on both ends in order for people to communicate. If that system isn't there and doesn't allow for that, then they just don't communicate. The new equipment we're producing now is such that we can move that key around electronically. However, there's still a tremendous inventory of equipment that's been out there for a number of years that requires someone to insert the key manually through a paper tape transfer or some other transfer device to get the key into the basic equipment.

NSDD 145 — what is it, and how did it come about? It was signed in September 1984. It was based on the biannual report of the National Communications Security Committee that was provided to the President in 1983. If you look at the history of the national structure for communications security, you'll see that the national structure basically started soon after World War II, when President Truman set up the Defense Department. It was created under the National Security Act of 1947. It was about 1950 or 1951, under NSC-268, that we got a two-man committee structure that was to have oversight over communications security on a national basis. That was the Secretary of State and the Secretary of Defense, one of whom was to be executive agent. The story goes that Secretary of Defense Forrestal and Secretary of State Byrnes flipped a coin and Secretary Byrnes won, so Secretary Forrestal became the executive agent!

Now, since that time there have been a number of iterations at the national level as to what the national system looks like. Up until the Carter Administration it was that committee of two with the Secretary of Defense as the executive agent for communications security, and the NSA Director acting for the executive agent to do most of the day-to-day business. There was a National Communications Security Committee that was made up of the military departments, NSA, the Director of Central Intelligence (DCI), and a couple of civilian agencies that would do the policy-type work.

During the Carter Administration it was recognized that the problem was larger than that of just national security. The system had done very well for national security up through that point in time. But the threat that was beginning to be recognized as a national problem ran the gamut from national security information, which could be translated as classified information, to unclassified information. The Carter Administration established a new mechanism wherein Presidential Decision/NSC-24 (PD-24), which came out in November of 1977, divided the world in half. It retained the Secretary of Defense as executive agent for national security and national security-related information, but the Secretary of Commerce was made executive agent for the remaining business.

For a number of reasons, that structure never got off the ground. The Commerce effort floundered from the very beginning, basically because, in my opinion, it didn't have the necessary talent available to be able to pull off the job. The talent was in a very small corps of people who resided in NSA. Commerce never really took on the challenge, never got going. The whole system kind of floundered up through 1984 when NSDD 145 was put in. One of the problems was that, if you looked around, there was really nobody in charge. There was no focal point where you could go to find someone who had the authority actually to pull some things off. The other problem was that the systems in effect at the time made for a lot of hate and discontent. Each department is responsible for its own security. It's like buying insurance: A prudent person, no matter what his salary, will invest some part of that salary in insurance as a protection for his family, should something happen to him or to them.

In that budget process that General Donahue was talking about this morning, you can well imagine where communications security fell when you have those high rollers sitting down worrying about tanks, planes, and battleships. One might think it would have fallen somewhere just below them. In fact, it fell somewhere down around swimming pools and bowling alleys. There just wasn't much. There are some reasons for that; for one thing, it was expensive. If you looked at the way we were doing it, it turned out to be extremely expensive because you had to hook it to something else. I'll talk about that a little later.

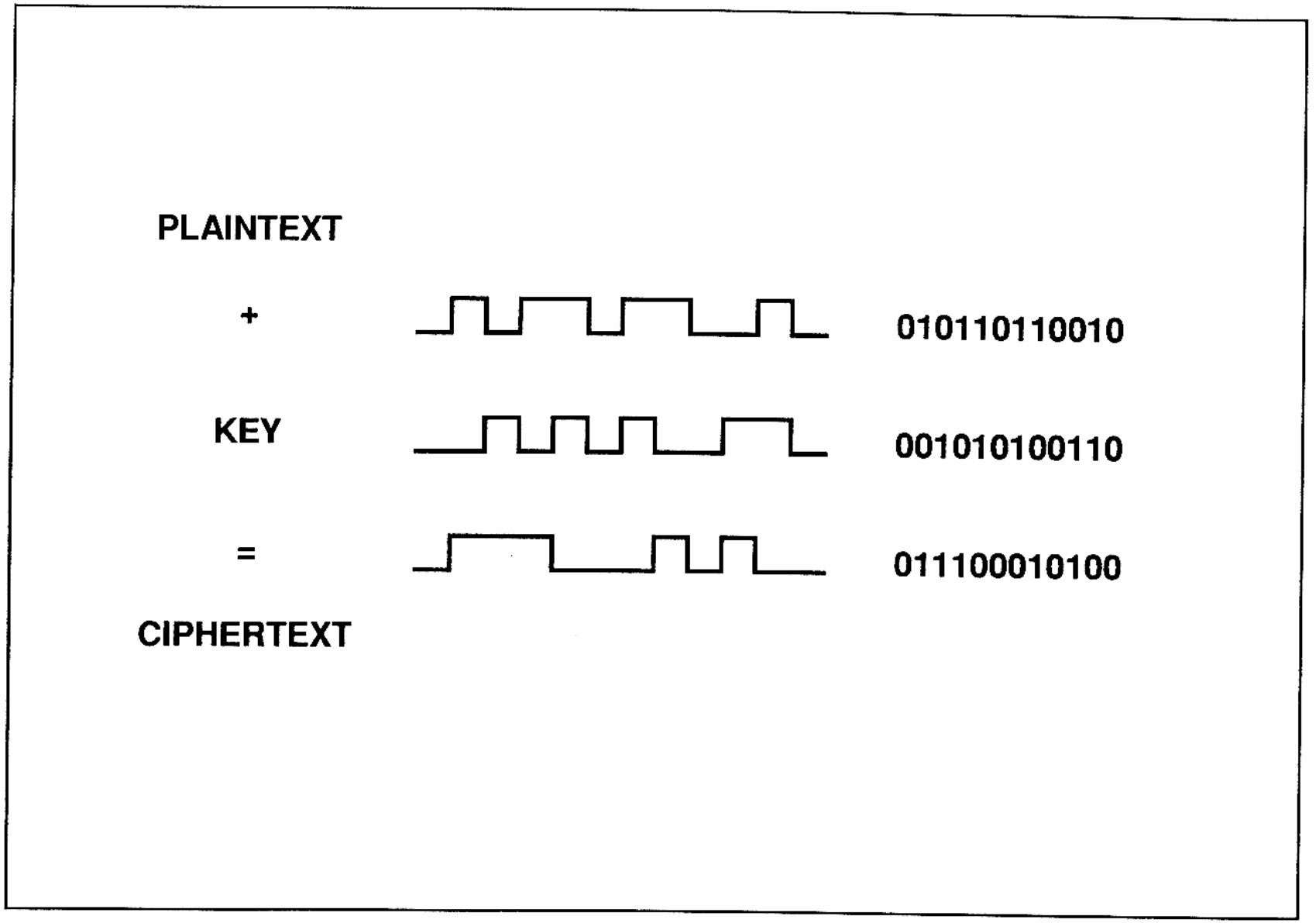

Figure 2. Production of Ciphertext

Oettinger: You mentioned that PD-24 came out under the Carter Administration in 1977. The ground work for much of that, of course, was laid in the Ford Administration, largely as a consequence of Nelson Rockefeller's interest in the subject. Given the fact that it arose as a matter of personal interest on the part of the then Vice President and eventually was sent around until it got translated into a presidential directive, one would expect fairly high-level concern about the subject, which makes it sound rather strange that it then became kind of an orphan. I think if you put that paradox in the context of some of the budgeting discussion in this morning's session with General Donahue, you get a sense of the operations of the U.S. government — or of any large entity, for that matter — where the titular head, whether it's the President of the United States or the Chairman of the Board of General Motors or whatever, has a great deal of prestige and in some respects a great deal of authority, but not necessarily a whole lot of money. So the fact that something is directed from the board room or through a presidential directive does not necessarily mean it will get implemented. This issue of he who has the gold rules, and exactly what and where the gold is, becomes very, very critical; as this example very poignantly points out, even something that is decreed by presidential directive is or is not worth the paper that it's printed on, depending on where the control of the money is with regard to the particular problem.

As for the question of why the arrangement with Commerce and so on didn't work out all that well, I suppose there are a lot of reasons for it, but let me give one that you did not mention. Mixed in with the question of where the talent resides was also a certain measure of perfectionism. I was hoping you might discuss a bit later the question of how gradations of protection in this area, or tailoring protection to perceptions of value, threat, and vulnerability, might be done. There's an old French saying, "The best is the enemy of the good." When one seeks perfection, and perfection is not attainable or is very expensive, then one tends to say, "I can't do anything." One could argue that yes, some of the knowledge resided in NSA, as you pointed out, but one could also argue that some of the perfectionism resided there as well, and the best became the enemy of the good. The whole effort, then, never quite got off the ground because of this question of what you do in between if you can't be perfect, especially when there's a certain amount of emotion involved.

Daniels: I think NSA "met the enemy and they was us." That was part of the problem.

Donahue: I'd like to go back to the Golden Rule, to give some credit. Based on pictures that the National Security Agency gave, hundreds of millions of dollars were taken out of the appropriations and put into the COMSEC arena. I think that, except for one minor glitch that we have in one set of equipment, on a principal basis, the Army has taken a lead in supporting COMSEC and making gains in that area.

Daniels: I think the situation today is not like the situation I'm describing. I'm talking about the situation of the late 1970s or early 1980s, when one of the big problems was that you had nobody in charge. You had a situation wherein the Secretary of Defense supposedly was executive agent for the national security and national security-related information, which took care of defense, and then you had Commerce in charge of the rest.

When budget time comes, with the Program Objective Memorandum (POM) process that Bob Donahue was talking about this morning — each service submits a POM, and out of those the Department of Defense creates a five-year defense program — the Secretary of Defense could ensure that at least the Defense side of this national security/national security-related realm had some importance in the budget. You'd have one budget review in Commerce and a simple look at it in Congress (basically, the House Appropriations Committee and the House Armed Services Committee, and then the Senate Appropriations Committee and the Senate Armed Services Committee) and then a review in the Defense Resources Board process. That would take care of Defense. But how about State, Energy, Treasury, all the departments that have national security information — where are their programs? They have one-year programs; they do one-year budgeting. There is nothing that takes you out in time as on the Defense side. Those programs are all looked at by a number of other committees in Congress; when you get down there on the Hill, especially into the subcommittees, the number of committees just grows and grows and grows and there's no one looking at the whole thing. Nobody!

You didn't have anybody at the presidential level any more because they did away with oversight by the National Security Council (NSC) since PD-24 brought it all down into the National Communications Security Committee, which was really run by low-

level guys. They were supposed to meet at least once a year. The highest ranking person who ever went there was the NSA Director. The other guys just never attended.

Oettinger: One of the concomitants was that Carter abolished the Office of Telecommunications Policy (OTP), and there was essentially no place left above the Secretarial level to look at these things.

Daniels: Now, the structure under NSDD 145 is that there is a system security steering group that is chaired by the National Security Advisor to the President, currently Admiral Poindexter (figure 3). On it are the Secretary of Defense, the Secretary of State, the Secretary of the Treasury, the DCI, the Attorney General, and the Director of the Office of Management and Budget. So you've got the money man, the legal man, the intelligence guy, and the two major departments, and the NSC is in charge. The Secretary of Defense is now executive agent for the entire problem. There is no role for Commerce anymore. There is also established a new function called "national manager," who is the NSA Director. The committee is now called the National Telecommunications and Information Systems Security Committee (NTISSC), chaired by the Assistant Secretary of Defense for C^3I, currently Don Latham. It's made up of the military departments, plus now the Joint Chiefs of Staff, and the major civilian components of the government. I think there are 20 members of that today. It's a working body with two major permanent subcommittees, one for COMSEC and one for COMPUSEC.

Donahue: It's at the senior level. I have to get written permission from Don Latham to attend if General Doyle* doesn't go.

Daniels: That's what's different from before. It meets four times a year as well, so it's looking at ongoing problems. What comes out of it is policy.

The national manager is charged under this NSDD 145 to prepare for the NTISSC an annual review of the state of COMSEC and COMPUSEC within the nation, which the NTISSC then submits through the executive agent to the steering group. The steering group will then meet and act on it. By charter, they have to meet once a year. The other thing that NSDD 145 did was to recognize that communications and computers were coming together and to make the NSA Director and the Secretary of Defense the national manager and executive agent, respectively, not only for telecommunications but also for automated information systems. So computer security and communications security are now driven by the same national mechanism. The Director of NSA is national manager for both.

The next diagram shows you the many ways of looking at information security (figure 4). When you come into the center it's all information systems: data, text, voice, and image. That's the problem.

What has the government done since NSDD 145? Why should things be better? Well, the first thing we've done is to embed cryptography. As this explosion keeps going on in telecommunications, you really can't keep up with it if you're trying to build singular devices to hook onto somebody's communications. You just can't keep up with technology. So the thing to do, if you're going to make communications security ubiquitous, is to embed it into that device. Embedding it also has another advantage in that if a soldier goes and picks up his radio and the communications security is embedded in that radio, then he's going to take his security along with him. If you give him an option as to whether or not he has that security, he may well not take that option, and leave it in the vault and go in the clear.

Yet another advantage is that it's cheaper. The decision to embed the COMSEC into the new SINCGARS* B radio saved $300 per radio, just in parts alone. That doesn't take into consideration the savings from not having to cable that communications security to something the way the VINSON** is cabled to today's radio. At one time the Army had 326 different configurations on how to hook VINSONs to radios, depending upon whether they're in a tank, a jeep, a manpack, a helicopter, this, that, or another thing. That is a major cost. It turned out that the cost of having the security was three times the cost of buying the box. Buying the box was just the beginning.

Donahue: Plus the maintenance problem, because you never could figure out where the hell the trouble was.

Daniels: To show you the change we've made, our

*Lt. Gen. David K. Doyle, USA, Assistant Chief of Staff for Information Management.

*Single channel ground and air radio system.

**Secure voice modulator/demodulator.

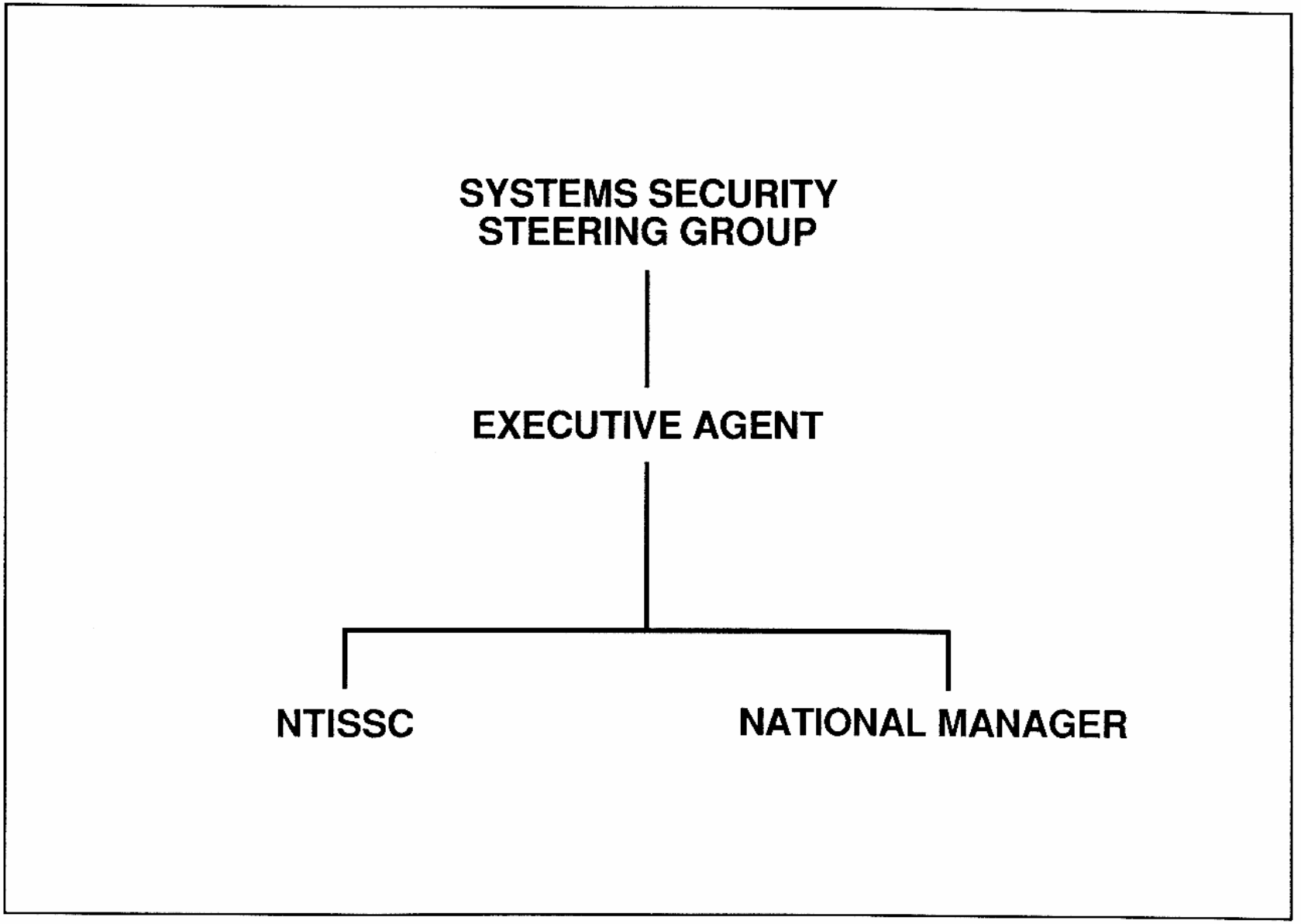

Figure 3. Communications Security Oversight Structure

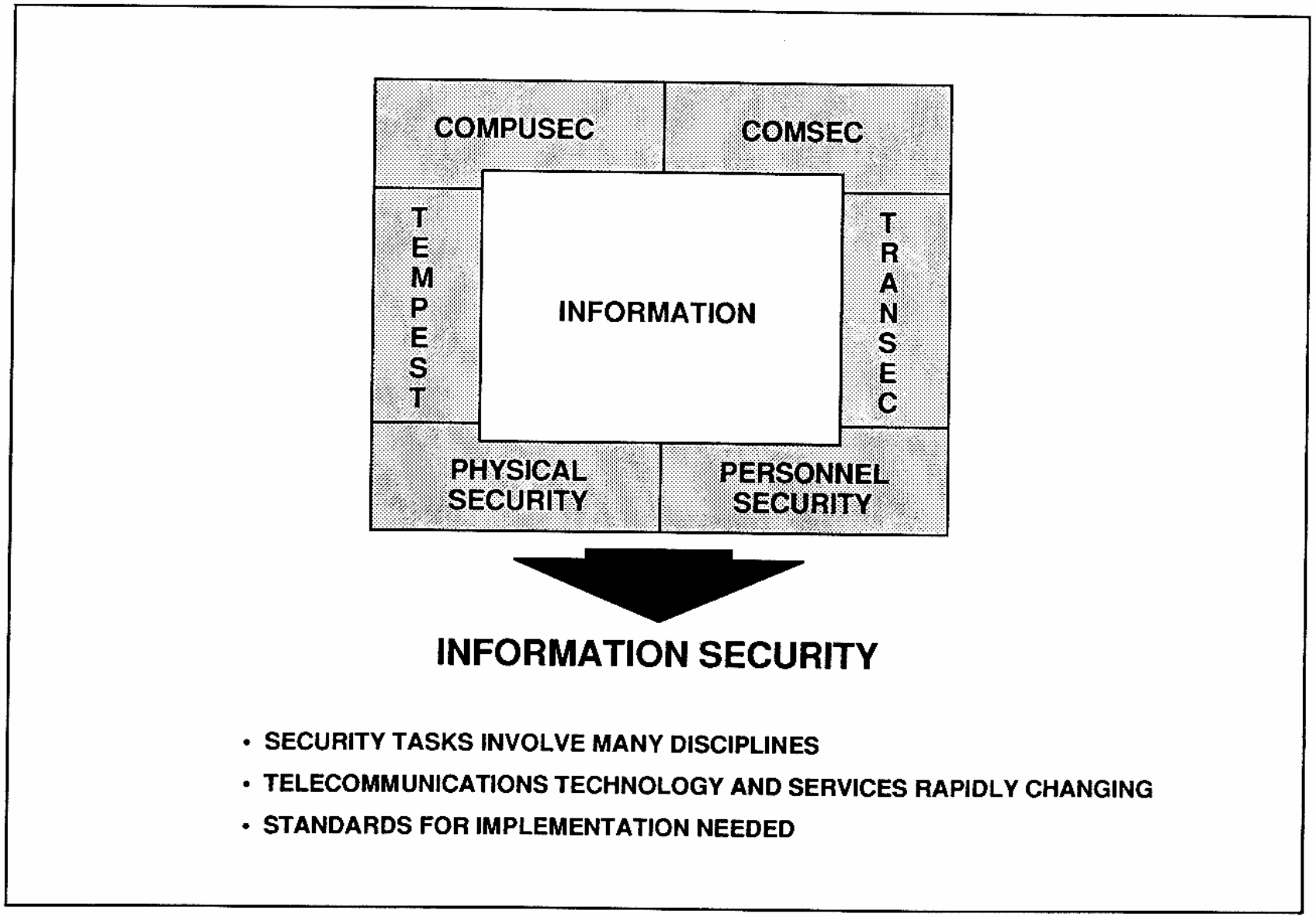

Figure 4. Information Security

traditional way of acquiring COMSEC was the hook-on method I just described (figure 5). You can look at that user terminal as a radio, a PC, or whatever you want to call it. Somewhere between you and it was this COMSEC device. That was the traditional way of doing things, not very user friendly. It turned out to be kind of expensive, was not transparent, and left you with a choice whether or not you wanted to use it. There is still, and will always be, a need for a general-purpose box for some kinds of applications, and some new general-purpose boxes are coming off the production line today. The goal is to try and move away from that traditional way of doing things.

The other big problem was in coordinating with the service construction of the radio. Let's say that there's a new Army radio coming out, and the Army says, "Okay, NSA, we would like you to build a crypto device that we can hook to this radio." In the old days, the way it was done was that they'd let a development contract to their contractor, and we'd let a development contract to our contractor. That development would end up in an engineering model that would then go into production. They would let a production contract; we would let a production contract. The hope had to be that somewhere down the line those two things would come together. If they didn't fool around too much with their system, and we didn't fool around too much with our system, it might even work! But that was not always the case. When things are in development and production, there is change along the way.

That problem should go away, now that we're headed toward embedding the COMSEC right into the unit (figure 6). It's being done today in the SINCGARS B radio, in the Air Force's miniature receive terminal, and in the Motorola hand-held radios or "bricks" that people walk around with. In order to take this new direction into the future, we have joined with industry in trying to set up a way to develop modules that will have standard interfaces such that we can publish in an unclassified way what those interfaces are, so any communications builder can leave a hole in his equipment for that embedded COMSEC module to fit into. What we did was to take a combination of corporations that had experience in chipbuilding — foundries and communications equipment builders — and some that had previous experience in building COMSEC.

Eleven of these guys have signed up (figure 7). That group has been in existence since last September, working right in our spaces to get standards that we hope will come out this spring.

Oettinger: At whose expense?

Daniels: Theirs and ours. It's a partnership. We're funding a little "seed" money for them and they're sending us their people.

The next major area where there has been some change is in the control. Previously, all COMSEC equipment was classified. It's usually classified either Confidential or Secret, most of it being Confidential. We have moved away from that and, in fact, declassified a great portion of the tactical equipment. That was one of the suggestions of General Donahue, and as a matter of fact, he can be regarded as the father of that.

Donahue: You couldn't build enough vaults to store it.

Oettinger: It's an interesting thing because one of the principles of cryptography is that the device should be out there and used, as after all the security is in the key, although we've never really lived by that dictum.

Daniels: That's been the theory, not the practice. Moreover, "Confidential" somehow seemed to make people think it was buying them something. In my opinion, all it was really buying them was nonuse of the equipment, because it was sitting in vaults. People were afraid to use it.

Donahue: If someone hands you a piece of paper classified Confidential, you know it's Confidential, but if they hand you a Confidential piece of NSA COMSEC stuff, the general reaction is, "Boy, I'd better not ever lose track of that thing," and the best way to do that is to keep it locked up tight. You can't get in trouble that way.

Daniels: Then you get to the very practical aspect of the problem. We decided that we were going to go embedded in order to make the COMSEC transparent and get people to use it. Now, are you going to classify the PC? Are you going to classify the radio?

Oettinger: Incidentally, this account is going down so smoothly, yet the moral equivalent of it is saying to some guy in AT&T that he's in the PC business, or having IBM buying Rolm or something. It's an enormous cultural change. If you want to look at a comparable transition in the unclassified world, you

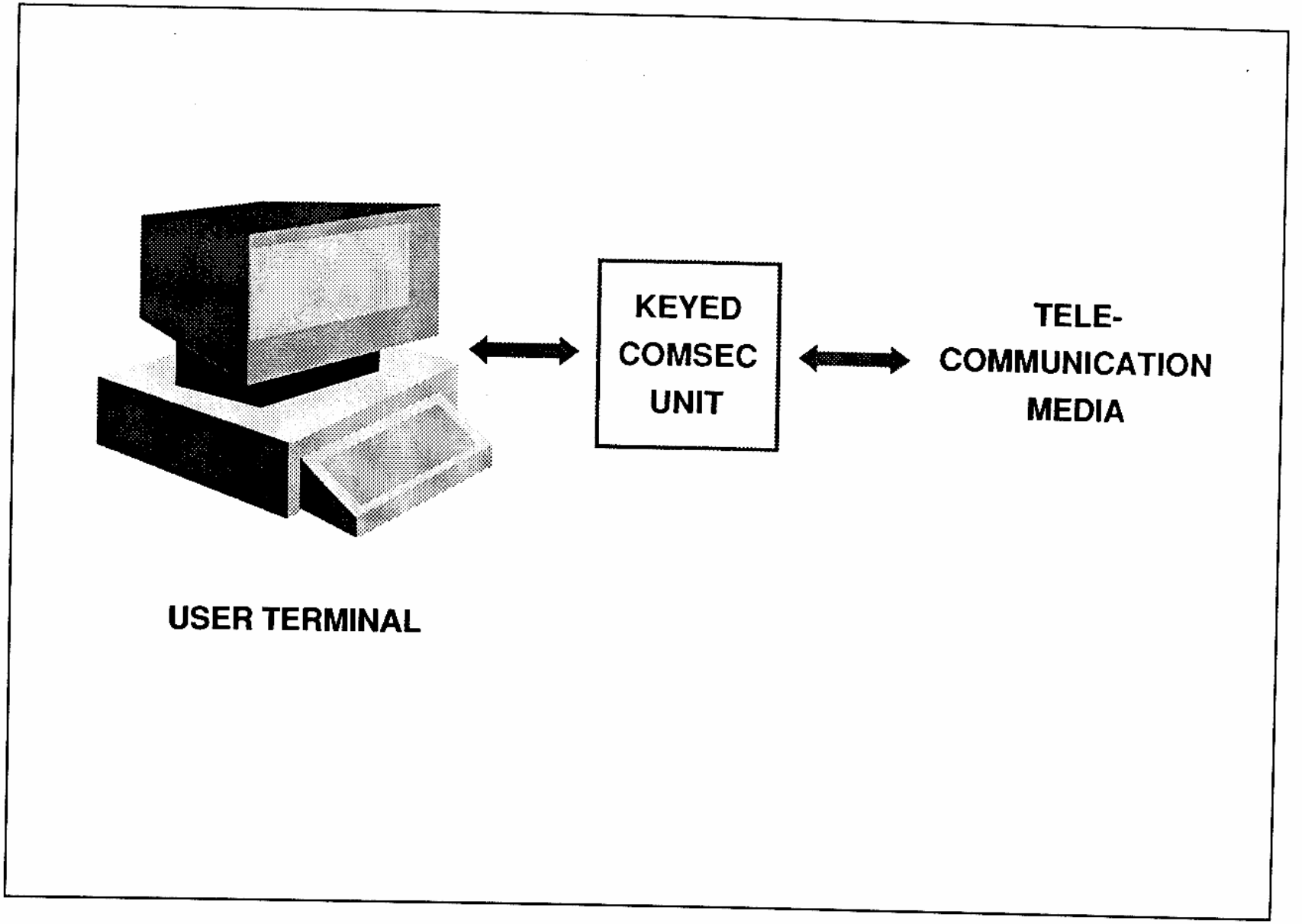

Figure 5. Stand-Alone COMSEC Application

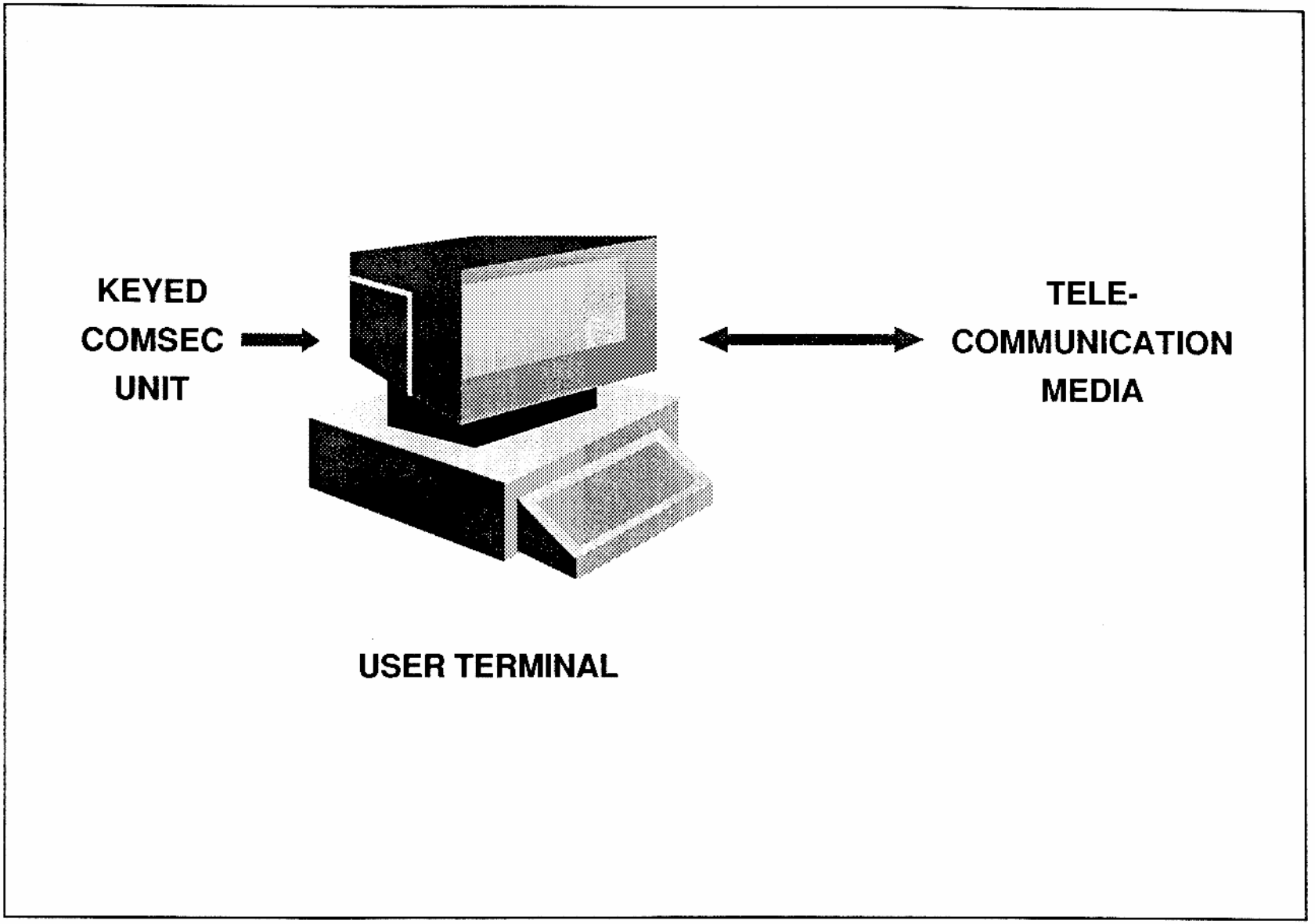

Figure 6. Embedded COMSEC Application

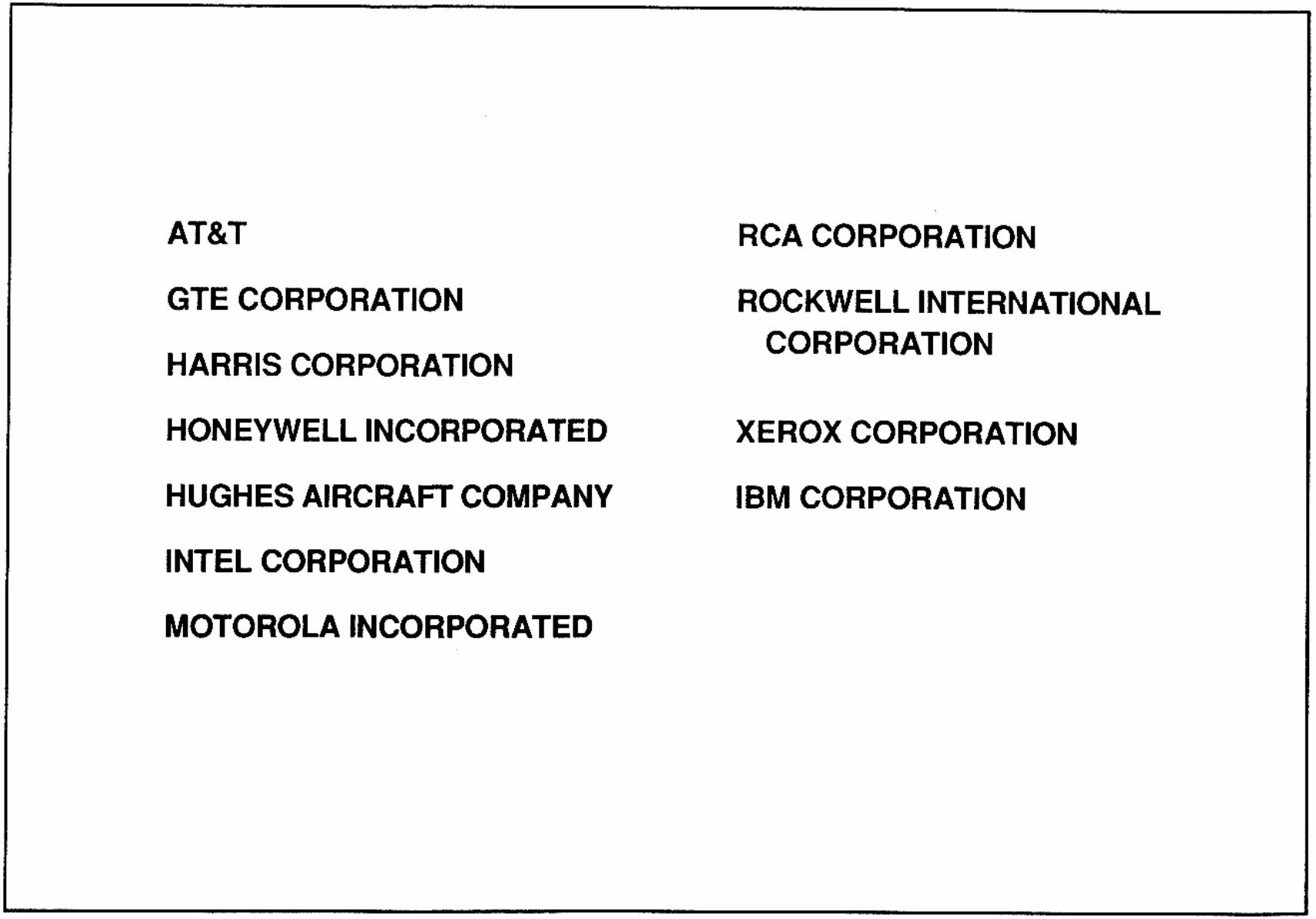

Figure 7. Corporate Members of the COMSEC Standards Team

should compare the 1985 statements of the lines of business of AT&T and IBM with each of their lines of business 10 years ago. Look at their annual reports. It's the only comparably massive cultural change I can think of.

Donahue: I have to give an unsolicited testimonial here. You spoke about the king not being able to implement his decisions — well, this thing was driven by Harry and Harry's boss, Walter Deeley, and nothing else. My major concern was that we wouldn't pull it off before Walter retired; the Benedictine monks would come back out of the basement again with their Rosary beads, and we would be back where we started. I was quite happy to find Harry being anointed as the follow-on, succeeding Walter as deputy director for communications security, so that we had continuity in this program. This is one case that would stand by itself and demonstrate that two people did make a difference.

McLaughlin: Let me ask Bob a question here. Actually it's in two parts. You talked this morning about how you were going to have 4,000 SINCGARS units through the division. Of course if you're going to keep that secure, that comes back again to the vault problem: If you're going to have that capability at squad level how can you keep it classified?

Donahue: You couldn't build storage vaults fast enough to cover my radios!

Oettinger: John, you see, you're being logical. The whole problem was an emotional one, not a logical one.

McLaughlin: Well, maybe while Bob is still here, I should ask the other SINCGARS question. I heard a tale about SINCGARS years ago in which one of the vendors was talking about the original plan to build a radio that was essentially a throw-away, step-on, $17 unit that could be mass-produced.

Daniels: The road to hell is paved with good intentions.

McLaughlin: As this vendor described it, 80 percent of the statement of work coming back was concerned with how you maintained it. The feeling among a lot of the vendors was that the maintenance tail in the Army wasn't about to have a throw-away, step-on radio.

Donahue: No, that's not true. In fact, that's getting into an area where we had an almost equal culture shock: There is a particular end-strength, and the Chief of Staff of the Army has said, "Thou shalt not break that." The other services have increased their end-strengths but the Chief says to maintain it, and there's only one way you can get any excess out if you don't take a shooter out, and that's to take a tail out. So everyone is in fact looking to reduce the requirement for maintenance support while preserving the fighting side. So any innovation that would come up that would reduce this requirement for maintenance-type personnel would clearly be accepted. It's a good story but I know it's not true today, and I'm not sure it was true the last time.

Daniels: I don't want you to get the impression that we were all nuts there for the last 30 years, because when we looked at the classification problem it seemed more emotional to me than real. What we decided we'd do is declassify but put controls on the equipment. We divided them into two other worlds, so we have three today (figure 8). We still have classified equipment, and for some specific things you need classified equipment. Then we have, for basically the tactical world, the controlled cryptographic item (CCI), which has serial number accountability with it just like your rifle, and the endorsed for unclassified item (EUCI). With CCI we have the same, if not better, controls today than we had when we were classified, and we get the best of both worlds: We get use, but we also have control. We know where they are. We know when they're missing. We have the Attorney General's guidance that even though it's not classified, if a piece of equipment is a controlled cryptographic item, we can still prosecute for espionage if someone takes one and sells it to the adversary.

Oettinger: I think a point worth underscoring is that while some of this may seem emotional and some of it may be seen as almost theological, the legal conundrums over the scope of application of classification, over the scope of authority in a given situation — for example, if it is not classified where does it fall under the Espionage Act? Where does it fall under what kind of legislation? — are matters of enormous importance in a society that takes its legal system reasonably seriously. If you get a little bit too loose in your interpretation of the law, it's quite possible that under different leadership even in the same administration, or certainly under a change of administration, what may have seemed like a good intention and a perfectly reasonable interpretation of a nebu-

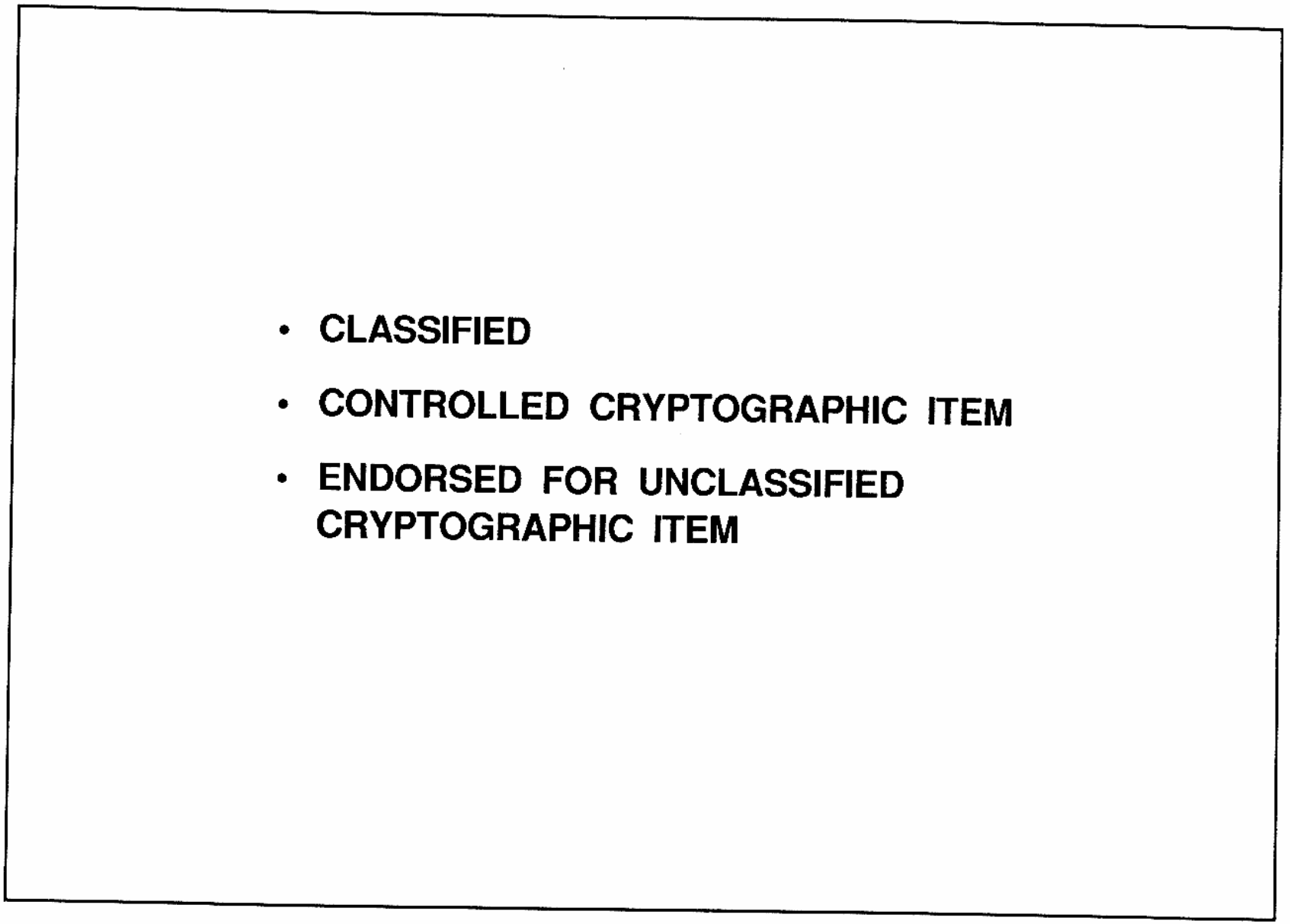

Figure 8. Equipment Controls

lous area of the law may get you prosecuted or thrown out of office or whatever for having acted beyond the powers of your office, and no prudent military or civilian officer would want to take a lot of personal risks in going beyond bounds of the law.

So this matter of adjudicating where the boundaries are, especially as you have done with these three categories, is sort of fascinating because you're spanning from the classified to the unclassified, and you're in a transition between the military national security world and the national interest/national security world, which ideologically and legally are two completely different worlds. There is an enormous achievement implied by that smooth-looking transition in those three items from top to bottom on that slide, which within the U.S. legal and cultural context is a fascinatingly enormous step to have taken.

Daniels: I should also mention a couple of other points. Something is CCI when unkeyed; if it's keyed then you treat it to the level of the key that's in it. If it's keyed Top Secret, then it's Top Secret while that key's in there. Then you can zeroize it and walk away from it and it's no longer Top Secret. That's the way we work that problem.

McLaughlin: Like a loose-leaf binder.

Daniels: Right. Also, we've limited access to U.S. citizens. Another point is that the third category, EUCI, takes care of the old Commerce problem and takes care of the private sector. It covers information that is endorsed for unclassified cryptographic items which have much less strict controls. It's quantity controlled, and it's always unclassified; you never have classified key for this kind of system. This shows the gradations of security, then, that one can achieve: You don't have to build all the bells and whistles into EUCI that you would into the CCI or the classified.

Student: Could you give specific examples for each of the levels? What kind of information would be classified, which might be more obvious, and what would be CCI or EUCI?

Daniels: It's a device I'm talking about here. You might have a device that you would use for a very specific purpose, where the purpose itself is very highly classified and compartmented, and the technology that you'd put into the device itself would be that way also. You also would not want to allow access to it by the general unclassified, uncleared person who would have access to the CCI. So a classified device might be something that somebody in the Central Intelligence Agency could use, or something along those lines.

Controlled cryptographic items are SINCGARS radio, the tactical radio, the hand-held radio, radios in airplanes, and things of that sort. Your endorsed for unclassified cryptographic item could be an IBM PC used in the financial community, or IBM PCs used in the Veterans Administration where they're trying to protect data that is unclassified but sensitive for purposes of privacy.

Student: The key would be there and would be used and not used depending on the situation?

Daniels: No, that's equipment now, okay? The key is a different thing. Both classified and CCI can take information ranging from unclassified all the way to Top Secret with 15 code words lying behind it. EUCI can never be used for classified information; it's just unclassified. You never get classified key for EUCI. People using CCI can order classified key and they will get classified key for their equipment.

Student: So the protection for the bottom category is therefore the multiplicity of keys, for the EUCI?

Daniels: EUCI applies to unclassified information.

Student: So what sort of protection is it then?

Daniels: You and your particular net will have your own key for that net. It's still protected by your key. If you protect your key, even though it's unclassified, you get full protection in it.

Oettinger: Keep in mind again that classified and unclassified are specialized words within the meaning of the National Security Act and the DOD deregulations that flow from that. One of the problems in this whole area has been in inventing the right terminology. Harry sort of fell into your question because he doesn't mean nonsecured in a colloquial sort of way. The information that some people hold very dear to their heart, like financial information in the Treasury Department or something, while not classified because it isn't covered by the National Security Act, may be worth a hell of a lot more than some pieces of military data. The whole business of inventing categories like sensitive, or extremely sensitive, or not so sensitive, or who gives a damn, whatever, that can be applied to such information is therefore a very important one. The point is, though, that under the existing legal structure it is not classified and we do not have a conventional, widely used system of

nomenclature for degrees of sensitivity in the unclassified world, which leads me to one other point I wanted to comment on.

EUCI takes care of the unclassified area in a kind of necessary but not sufficient way, in that it makes equipment like that available, but whether anybody would bother using it is a whole other matter. The incentives on the classified side have to do with the law. They have to do with the kind of details in military budgeting we were talking about back and forth with General Donahue. Whether a private sector enterprise would use any of this stuff, given an incremental cost, is a completely different question that we haven't talked about.

Daniels: Our job is not to be authoritarian in terms of "you will use." We're there to provide the system for your use. We're not defining sensitivity; users have to define that for themselves, and they do. If you go into the Department of Health and Human Services, you'll see that they have different classes of data bases, for example, that have different sensitivities in them. They call them one, two, and three. We call them Top Secret, Secret, and Confidential. The categories mean the same to them as they do to us; it's just not national security.

Student: Where does the data encryption standard (DES) fit in; under EUCI?

Daniels: Yes.

Those categories took care of the doctrinal aspects of things. Then we had to address what was, frankly, a business problem, in our relationships with our customer and with industry. The traditional way we did business was like what I described a little while ago, when they went down one road with their equipment and we went down another. The other problem with that approach was that when they went through their budgeting process, so much money was put against a particular item by the Army, Navy, and Air Force in their program. Then Congress would appropriate that money. Let's say the Army, Navy, and Air Force each have a dollar. NSA was the central procurer for the nation. In order to procure things you've got to have money. In the old system, the services would provide money to us through what is called the the MIPR process, which is an interdepartmental way of moving money around: military interdepartmental purchase request. When we got all those MIPRs together, then we could go out on contract. You can see the interesting part of that: You have to wait for the last guy in before you can go on contract. The Army sends its money in right off, the Air Force sends theirs in a little later, and the Navy hasn't got around to it yet. Once again you've got a system that's built with hate and discontent.

Another problem is that if you're in the third year of a three-year contract, and all of a sudden the Navy decides it doesn't want to be part of it any more and pulls its money out, then you have to renegotiate the whole damn contract and quantities have to go down and prices go up. It's a terrible situation.

What we decided to do was try and work with the services as a customer to get into a user partnership (figure 9). NSA appropriates all the research and development money for COMSEC. Even if it's embedded COMSEC, the money for the development of it comes from us. What we're going to do now is move our money into the services. We're going to reverse the process and start at the front end. We're going to help the services in the development cycle. I've actually got people at the SINCGARS program manager shop up at CECOM,* now at Fort Monmouth, working the SINCGARS problem. We've been pumping the money up there to them. The same applies to the PLARS/JTIDS** hybrid. The emphasis in this new approach is on the embedded systems. We'll still do the traditional ones the way we did before. That should really speed up the process and make sure that what comes out at the end is complete, not half of it sticking out someplace.

So that took care of the customer relationship. We also changed the way we dealt with the people in industry who were building these devices for us. Secretary Weinberger said, "Look, we're bleeding to death with unclassified technical information that is being passed between engineers, both between the government program manager and the company that's building for that program, and that corporation and its subs and its vendors. What I want to do within two years is make sure that I've protected not only all classified communications, which should have been protected before anyhow, but also those unclassified communications that would allow for a technology transfer." We said, "Gee, Mr. Secretary, that's nice, but under the traditional system you couldn't do that in 10 years, because you've got to go get money, you've got to

*Army Communications and Electronics Material Readiness Command.

**Precision Location Reporting System/Joint Tactical Information Distribution System.

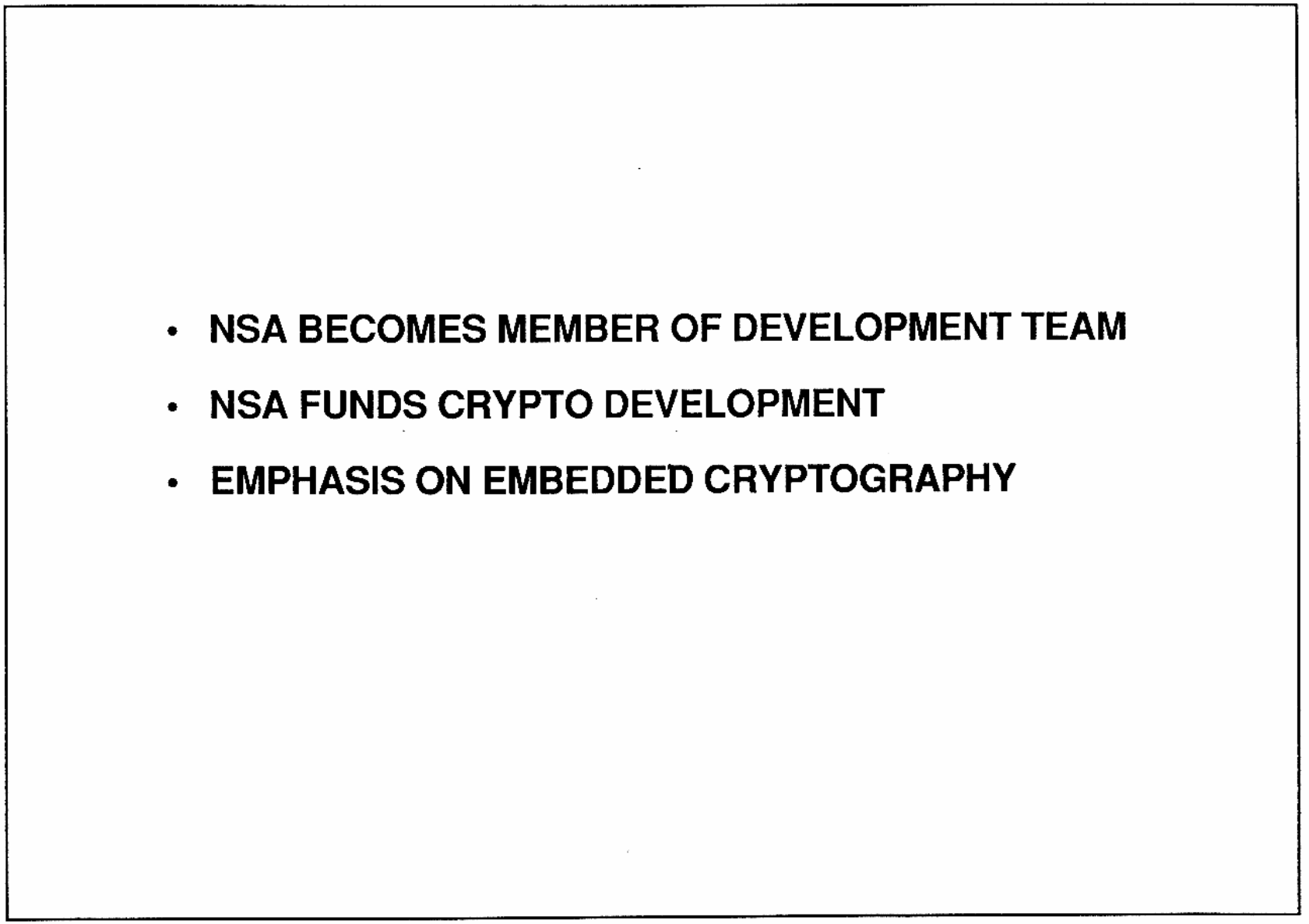

Figure 9. User Partnership

let contracts." As Bob Donahue told you this morning, two years after he gives me money, something comes out the other end.

We also looked at those people we had who were building stuff for us under the traditional method, and decided to make them authorized vendors so that the services can buy directly from them. Then we looked at going out to industry and saying, "How about joining us in a partnership and you build something with COMSEC in it — we'll bring our expertise to the table, which is the cryptographic expertise, and you bring your expertise to the table, which is power supplies, modems, and the things that industry does best." In the past, we used to invent modems, and we used to build power supplies, and casings, and other things that went with that traditional procurement; now we said, "Why don't you work with us and we'll help you build that in, and you get a value-added product that you can sell out in that marketplace." Under the use of the partnership, NSA becomes a member of that services development team.

So we embarked on a program using authorized COMSEC vendors (figure 10). We decided to take people who are currently building things for us and allow them, under certain controls, such as a memo of understanding (MOU) with them and legal prohibitions, to make direct sales now and do marketing. To give you some examples (figure 11) the KG-84 is a general-purpose data encryptor, and the KY-71 is a voice system that's in existence today; the KY-58 is the VINSON equipment, and the basic reason for that MOU is because the mobile subscriber equipment system, which the Army is buying as a nondevelopmental item, went to GTE and the French Thomson RITA system. And SDC/Burroughs is the contractor for the general purpose key inserter to go into those pieces of equipment.

Now if you're TRW and you want to tighten up your communications because you have Defense contracts, you can go directly to those people and buy that equipment. You can write it off as part of the normal security aspect of your contract, just like your three combination safes and your compartmented areas within your building. It's just a regular security thing.

Probably the most interesting program, and the one that's really going to get things going, is the Commercial COMSEC Endorsement Program (CCEP) (figure 12). That is, a vendor will come into NSA and say, "I see a market for a PC with encryption in it, and here's what I want to do." We get into an MOU with him whereby we tell him what the procedures are, the standards, and all of that. He provides engineering, design, and the equipment to us to actually test, and we give it the Good Housekeeping seal, our endorsement that says that equipment is secure. When we get some of these actually out on the street, soon there will appear something analogous to the General Services Administration (GSA) catalog, wherein one can look and find an evaluated products list that says these companies produce secure PCs at these prices.

Oettinger: I'd like to make a background comment on what you're looking at here. Harry presents this notion as if it were the most natural thing in the world, which in the political climate of 1986 is a perfectly reasonable thing to do. Ten years ago, shortly after Watergate and Nixon's departure, the question of endorsement by NSA, or for that matter of any aspect of the military being the sole keepers of things having to do with the private sector, etc., was not exactly something that anybody would buy. Part of the reason for the peculiar setup that Harry described earlier was that the Carter Administration came in cleaning out a number of Nixon/Ford kind of things. The Office of Telecommunications Policy had acquired an image of messing around with the television business, partly through some of Clay Whitehead's unfortunate speeches in those days when he was head of OTP. The new administration brought in the notion that there had to be some civilian input if there was influence on the civilian side; hence the Commerce Department involvement.

As for the notion of certification and so on, even four or five years ago NSA's role in the data encryption standard still raised questions publicly debated all over the place that the whole thing might be simply a scheme on NSA's part to control the cryptography in order for it to be able to access the systems. It was five years ago when that kind of debate was raging.

So there was a combination of technical complexities, cultural questions within the communications security problem, and the external political climate that I just indicated a couple of moments ago. If you then wonder why it takes 10 years or more from an enunciation of a problem by the then Vice President to getting this kind of development fielded, I think you begin to get some of the reasons in Harry's account. You're seeing in this

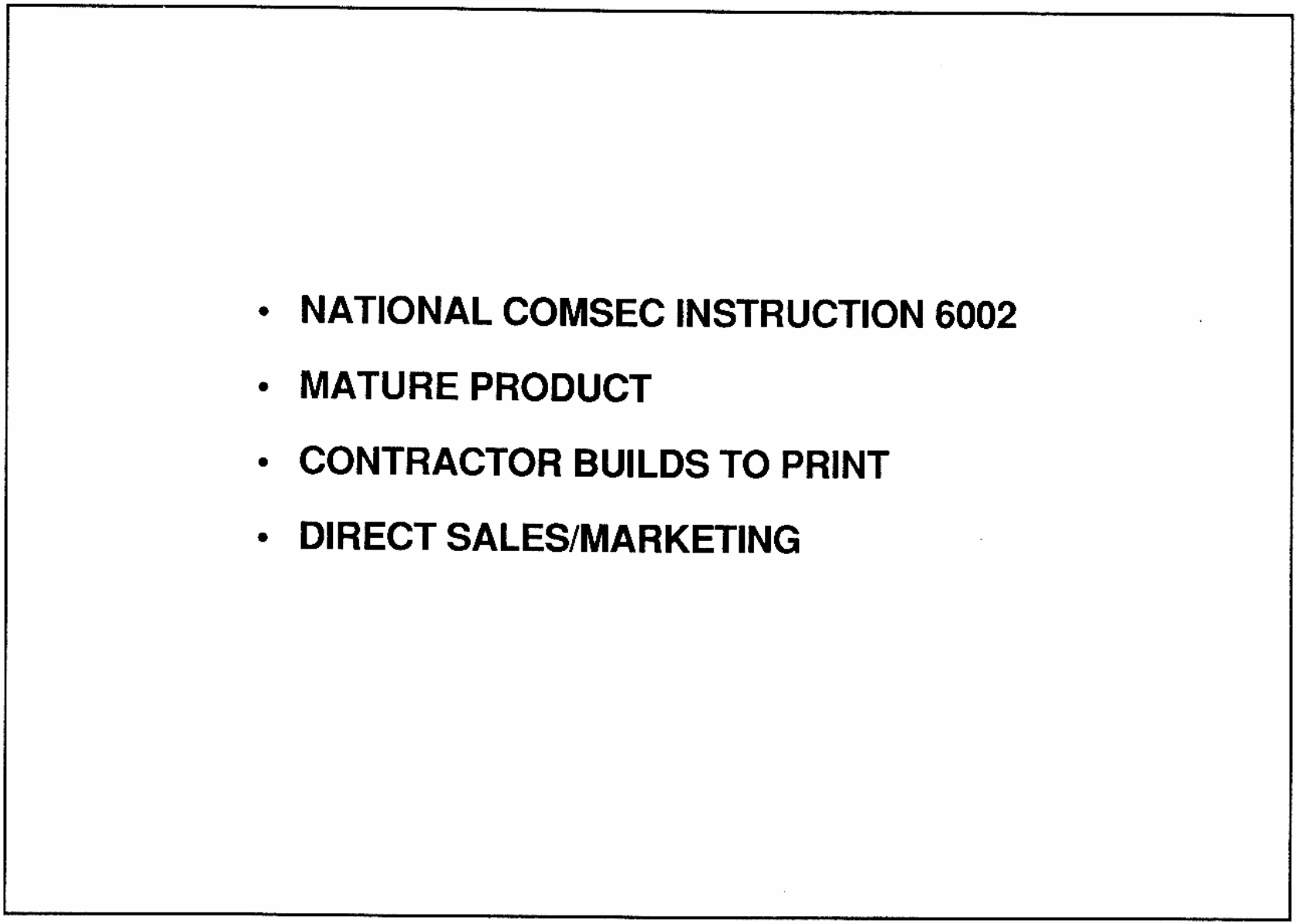

Figure 10. Authorized COMSEC Vendors

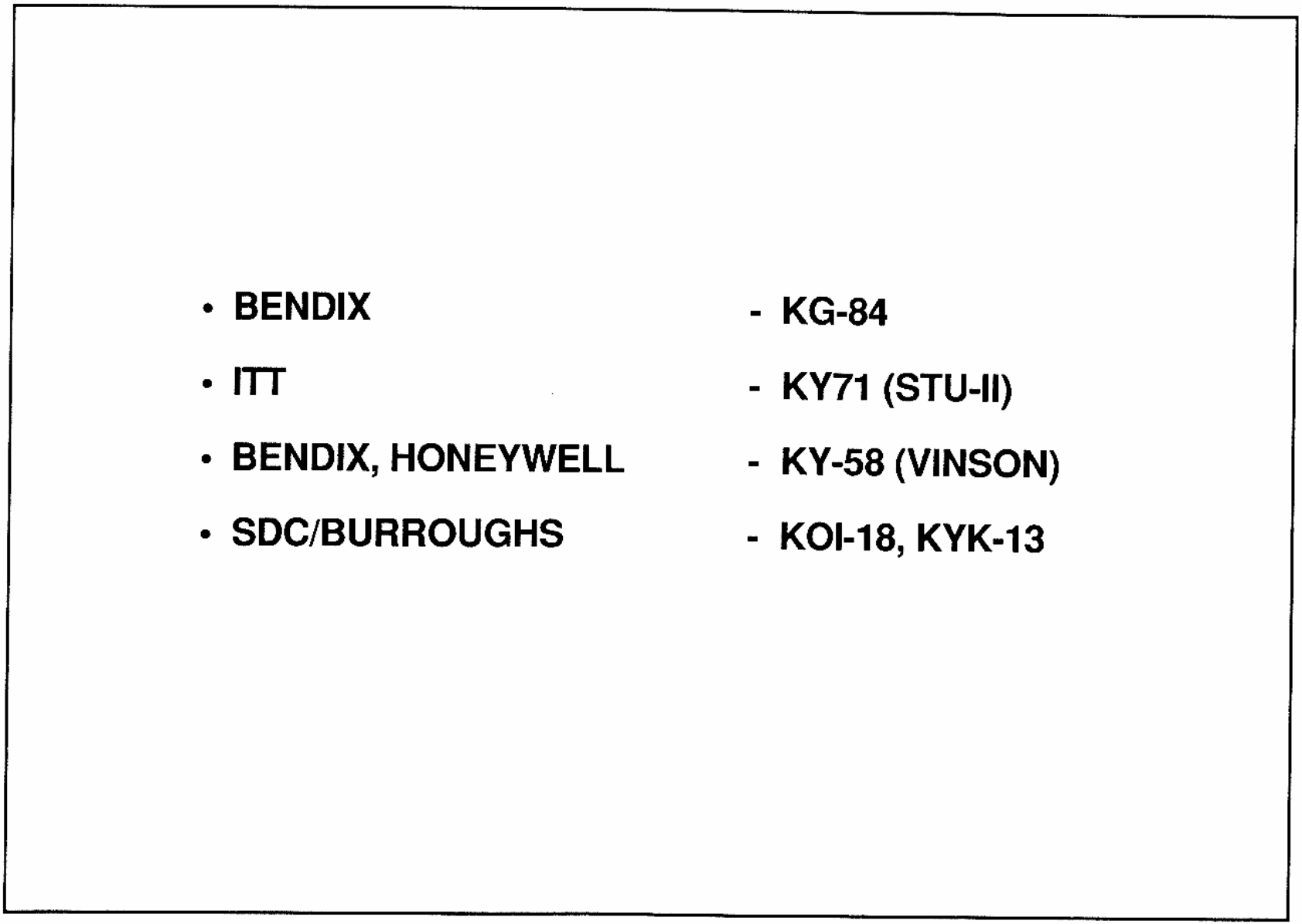

Figure 11. Authorized COMSEC Vendors — List

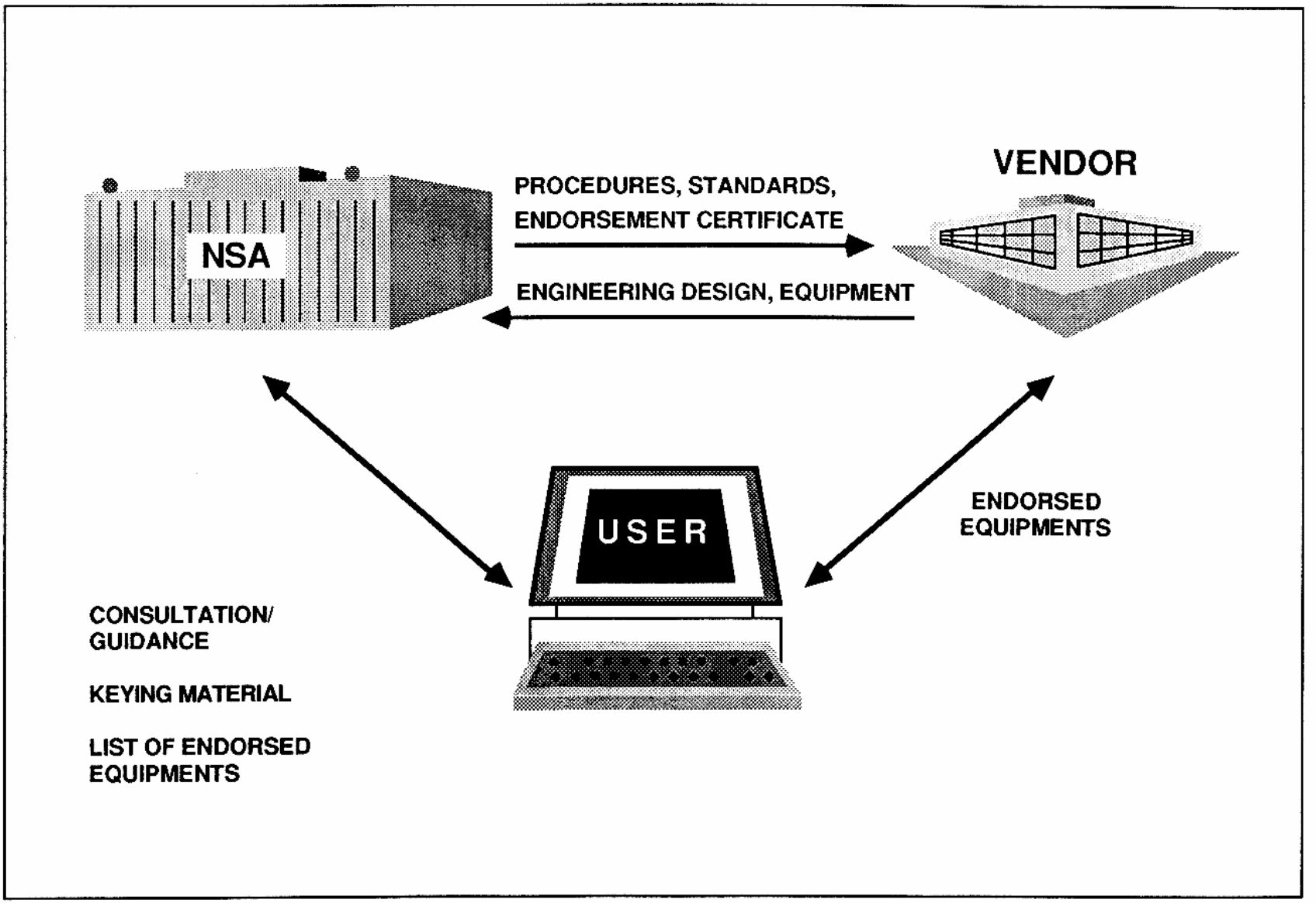

Figure 12. Commercial COMSEC Endorsement Program

microcosm a blend of a whole range of factors that intervenes in this path from noticing a problem to doing something about it, accounting for why it sometimes takes time in the translation from laboratory possibility to real-world deployment.

Student: To what extent would your contribution help accelerate movement toward electronic check and fund clearing by the financial industry?

Daniels: We're already providing for the Treasury to do that; in fact, the Treasury's doing it with DES. All electronic funds transfers (EFTs) are going to be encrypted for authentication. It's Treasury policy now.

One point I wanted to make here was on the keying material. This comes back to your NSA-as-Big-Brother approach: For all government customers, of course, NSA is offering to provide the keying material, but as far as the private sector is concerned, we will provide keying material at cost or you can develop your own. That particular approach allows you then either to come into NSA or to do your own thing if you don't trust us for some reason. Why you wouldn't, I don't know. Some might not.

Here's an idea of some of the CCEP programs that are coming up (figure 13). Of the people who are signed up with us now with MOUs, about one third of them have proceeded beyond the MOU stage toward a memorandum of agreement where we've actually got specifics on these things. They've got schedules, and you should see some of these products within six months to a year. The data encryption and authentication item is one that could be used in the EFT world. We're also looking to secure local area networks and PCs; a lot of people are getting interested in that field. The purpose of the satellite telemetry and control program is so that nobody can take your satellite and move it.

One especially interesting one is the secure telephone; that's being done by AT&T, RCA, and Motorola. It is not a completely CCEP-type program, but pretty darn close. Today we have what is called the STU II. You may see it on the desk as a little device, but behind it stands a 70-pound monster. It's 1970s technology. It started with costs of around $32,000 apiece; in the last contract we let, they're about $10,000 to $11,000. That's because we had quantities. We felt we could never get the price down below that $10,000–$11,000, and it's not too user friendly. It takes two telephone lines into your system. You have to go through a key distribution center, so you really have to make three calls. You're not actually making all three, but after your one call it makes two others to go get the key and bring it back. The key distribution center it had with it would hold up to about 20,000 units at the most.

We decided that we wanted something that cost no more than $2,000; that looked, felt, and acted like a telephone but used one line; that was modular; that you could plug in just like your telephone at home; and that had all the modern features of a telephone. We went out to the big telephone makers, AT&T, GTE, RCA, ITT, and Motorola — Motorola basically because they're very big in the cellular business. We said, here's what we'd like to do. Here's where the government can help drive the market in the private sector: We see a market in the government for about 500,000 of these things, about 200,000 for classified types of conversations and about 300,000 for that nonclassified but sensitive world. We guessed, based upon some surveying we'd done, the private sector would buy about 500,000 more if they could buy them at this price.

Each one of those companies went out and did their own market survey. Interestingly enough, it's all tied to price, but if you get down here around $2,000 that private sector market is over two million. That's what they said they'd buy. That doesn't mean they will, but the market survey showed that's what they'd buy. Those companies put a lot of their own money into development. This time we did not give them the typical government specifications; this is where it tends to be more like a CCEP thing. We said, here's the performance we want. They built to that performance.

Three of them won: AT&T, RCA, and Motorola. The military had a requirement for something that would be used in a command and control kind of operation, which had to have some more things than your normal telephone. RCA was building something for us already in the secure mobile unit, so we transferred that technology into what is now called the STU III technology. This militarized version sells for about $7,500. You can see what it costs you to militarize something.

To show you how fast this went, we went out a year ago with the contracts and the first prototypes will be available in June. We'll have models from

PRODUCT LINE	COMPANY
PCs	AT&T, IBM, Zenith, Systematic General, GRiD, PE Systems, HP, Analytics Communications Systems
LANs	WU, Xerox, Sytek, DEC
Data Encryption/ Authentification	Motorola, E-Systems, Martin Marietta, Honeywell
Radios	Motorola, Magnavox, RCA
Satellite T&C	RCA, Hughes
Secure Telephone	AT&T, RCA, Motorola
IFF	Hazeltine, Bendix, Teledyne

Figure 13. Sample CCEP Programs

each one of these companies available for testing in August. We'll start production in June of 1987. Each one of these guys has a capacity to build 10,000 a month. They're coming in at around the $2,000 cost and they're on schedule. That shows you what you can do when you work with people who know how to use the technology. It's their business, and all you're doing is bringing to the table the cryptography to go into the thing, rather than giving them six million specifications to work against, which take seven years in development and three more years in production; and you bring it in at a low price. That is the only way, in my view, that you're going to get that or get the marketplace developed. You're not going to get a guy with sensitive information who doesn't really understand the value of his material to protect it if it costs him an exorbitant amount. Most people, I think, will pay somewhere between 7 to 10 percent more for their communications to get it protected.

Oettinger: They might. Let me just make a comment on that for a moment, because going back to your earlier discussion about value, vulnerability and threats, it seems to me that at a $2,000 cost you have a lower threshold of the combination of value, vulnerability, and threat for somebody to come in. Your statement that more folks will come in at that price than if they had to pay $30,000 is obviously true. Whether that's enough or not from some public point of view remains to be seen. There are folks, for instance, in the department store or food store business who are happy to tolerate fairly high shoplifting rates because the alternative is not palatable for them in that kind of business. It seems to me the situation is somewhat like that in fire protection and so on, where, at the other end from what is done by ordinance, some of it isn't done at all. We recently had a smoke incident in one of our skyscrapers here where there weren't sprinklers, etc., etc., because the Prudential was built before the ordinances on sprinklers and on chemical fire extinguishers. You have a situation where folks won't buy a fire-retardant safe or one thing or another unless what they're buying is subject to Underwriters Labs rules and they can't get insurance otherwise.

Daniels: That's a big driver.

Oettinger: Is there, in this bag of tricks that you've got, something like the Underwriters rules and so on that would bridge the gap between the $2,000 threshold and what from a public point of view might be regarded as a desirable level of protection?

Daniels: You're beginning to see that as a natural phenomenon of the insurance business. They're beginning now to go to these guys who are losing money as a part of doing business and they're raising their insurance rates. If we can work with the insurance company and say well, if the guy is protected, then you ought to be able to give him a better insurance rate, then those kinds of things are going to be drivers. The bottom line is the buck, no matter what you look at.

Student: How do you monitor loss from communications leakage?

Daniels: You can see the hacker getting at you. You may not see it when it's happening, but you find out after the fact that the hacker's been in there and done something to you. The case at the Sloan Kettering Institute in 1984 could have been disastrous.

Student: What does the FBI think of this? I'm thinking of people whom the government might want to surveil who might want to guard their communications from each other or from the government.

Daniels: We wrote it off. It's a risk assessment thing. We're bleeding to death today with hardly anything being covered the way it should be. In order to get ubiquitous COMSEC out there, you're going to take a little loss. You weigh that risk and say well, the gain is going to be worse than the loss, and there you are.

Student: Do you contemplate a control for the sale of these?

Daniels: There are some controls on them. I am not about to sit here and say one will never get away from me.

Student: Sure, like a handgun.

Daniels: We will have sales somewhat patterned after handguns. At the point of sale you have a history of it, but that doesn't mean it might not work its way in to undesirable hands. You have to start somewhere.

Student: What would be the policy on exporting such equipment?

Daniels: The policy is no export.

Student: Because here I see a dilemma. On the one hand you want to control the exchange of information with your allies; if you don't have this equipment, then there's a problem of security in this information exchange. On the other hand, if you have the controls through such equipment then there's a possible danger in that the equipment itself may become available to the other side.

Daniels: We have controls on export built into this system. That doesn't mean that, when it's in the government's best interest, you wouldn't export it to some of your allies for use in interoperability. We've done that in the past. NATO, for example, is a heavy user of U.S. COMSEC. What we won't allow is for these vendors to sell directly. They'll have to come through the government.

Student: But you won't be able to prevent it from ending up wherever.

Daniels: These all come under the International Traffic in Arms Regulation; all cryptography is treated like weapons and comes under the Munitions Control portion of that export regulation.

Student: Another thing that struck me: On the tactical level, with 4,000 pieces of equipment in a division, what happens when the first piece of equipment is lost or whatever? How do you protect the crypto thing against falling into the hands of foreign adversaries?

Daniels: You don't. You expect losses in battle. That's why it's always been the approach that when we build this stuff we build it knowing we're going to lose some. We put the confidence in the keying material. We change the keying material periodically; we can change it monthly, daily, hourly, however often you want to change it. When you lose one, you take that fellow out of the net. He doesn't get rekeyed, he's gone.

Oettinger: As I pointed out earlier, it has always been the theory that good cryptography requires a system such that even if the system's compromised it doesn't matter as long as the key isn't — you change the key or whatever. That rarely, if ever, has been the doctrine in practice. I think what Harry is saying is that there is a major cultural change afoot that says that you begin to do in practice what is always supposed to have been the normal theory.

Student: You mean the system is tracked to such an extent that it will never be compromised?

Daniels: No. I can't tell you that. It will be compromised. We've got a case right now, a fellow by the name of Walker, who was in the Navy and who did compromise us.

Let me just tell you what I mean by a key generator. The key generator has plain text coming in, and cipher text coming out. This key generator develops a random string. The key that I'm talking about is another variable that you add to that. The guy who steals the equipment will have the key generator but he won't have the keying material. So as long as I'm using different variables on what I've still got left, it's still secure. That's the theory behind that key, and that's how it really works. Now, if somebody steals this key and has got the generator, you're compromised. The point is that you've got to give heavy protection to the keying variables. We talked about declassifying some of the equipment. We've now got even stronger controls than we've ever had, though, on the keying material because we have reduced our controls on the equipment. In some cases we have two-man control on the keying material. Two people always have to be there with it; one person can never be alone with it so that he can put it on the Xerox machine and copy it. Controls have gotten much stricter. Keying material is still highly classified.

Student: Isn't there a vulnerability about distributing the key to the terminals?

Daniels: To the terminals? Once again you've got cleared personnel. If it's Secret key it can only be handled by Secret cleared people. We're putting in controls on the Top Secret stuff such that it has to have two Top Secret cleared people with it. If your security clearance system is working, you've got trustworthy people carrying the key around. What I want to do is get away from the system where somebody must physically carry the key to this key generator and insert it with either one of those insertion devices or a tape reader or something, and get it out over the air to somebody else in an encrypted form. Rather, it will be encrypted in NSA, and go over the air and right into the key generator in encrypted form and be decrypted at the other end.

Student: That's what I'm wondering about. How do you secure access to the key generators?

Daniels: We're doing that. We're doing that on the STU III; we have that capability on the KG-84, and all the new equipment coming out will have an over-the-air encrypted key going with it. It's for that old stuff out there like the VINSONs and the other things that you've still got to carry manual key around and insert it. That's where the Walkers get you.

Oettinger: So again, it's a matter of "compared to what?" It may have some holes left, but in the old days Walker and the like compromised you with manual key.

Student: What about taking the implications one step upstream: In certain messages, over and above the telegraphy there are certain link standards or protocols to be protected because they describe how you organize the data bits that are sent, and even that is classified. You don't want people to know how those links work. At one stage both the key and the keying generator were considered as two levels of protection. If you now concentrate more on the keying material itself, will that change the classification in this new approach in terms of protocols?

Daniels: No, not necessarily. You can and do have unclassified protocols for people to communicate, and then we will be putting out standards so that the cryptography that's embedded in the system will never inhibit you from interoperability. So if you've got one kind of system and it's interoperable with another, those embedded COMSEC devices won't inhibit that interoperability. Of course, they won't enhance it, either. If you've got two units that don't talk together now because of their communications protocols, they won't talk together after you put in the cryptography, either.

I told you I'd pass along my own views about the industry side of the world. I guess what I've got to say comes down to three points. First, in my view, information is becoming more and more vulnerable. We are moving into a service society with the hollowing of American industry. Second, there's a tremendous opportunity for technology transfer out there because of the communications explosion.

McLaughlin: Harry, what do you mean by the hollowing of American industry?

Daniels: American industry is not now building its own stuff. It's going offshore to get material, and what we've got now, instead of matrix organization, is kind of a network organization where stuff is coming in from here, there, and another place, and all we're doing is putting it together.

To show you what I mean, this chart (figure 14) indicates that from 1880 on up until about the year 2000, if we look at the distribution of the U.S. work force, you'll see that agriculture has come way down; industry's come way down; service is up, but flattening out; and information's going sky high. So, we seem to be an information society today. I think business is going to have to come to terms with the problem and learn to understand and be aware of their vulnerabilities and the threats against them. The government is there to assist them in protection, but we don't legislate it. We're there at their call.

That basically concludes my prepared remarks.

Student: Those beautiful encrypted telephone machines that you showed us — are you aware of the possibility that six months or a year later the Japanese will come out with the same thing at half the price?

Daniels: Yes, but I won't endorse it.

Oettinger: That's an interesting point. You won't endorse it until the U.S. Trade Representative and the Secretary of Defense have words.

Daniels: I could never see myself endorsing a Japanese crypto device for use in protecting U.S. information. It gets back to the problem of losing one. Private business can buy it; I just won't endorse it.

Oettinger: It's just like electrical equipment, which is where the insurance industry comes in. You can buy electrical equipment that is not certified by the Underwriters Laboratory. If you are a private citizen and you want to put a toaster in your house that's not certified by the Underwriters Laboratory, nobody can bother you. The first time your house burns down and the investigators discover that toaster and somebody gives a damn, your insurance price next time will go up. If you're the XYZ Corporation and the insurance inspectors come around before they sell you the policy, and you have unendorsed Japanese something-or-other, they may not write you an insurance policy.

Daniels: This endorsement program is not new. There's all kinds of junk in COMSEC out there today. You can buy a lot of cryptography all over the United States. We were talking about the data encryption standard a little while ago. There is a standard for endorsement of that (Federal Standard

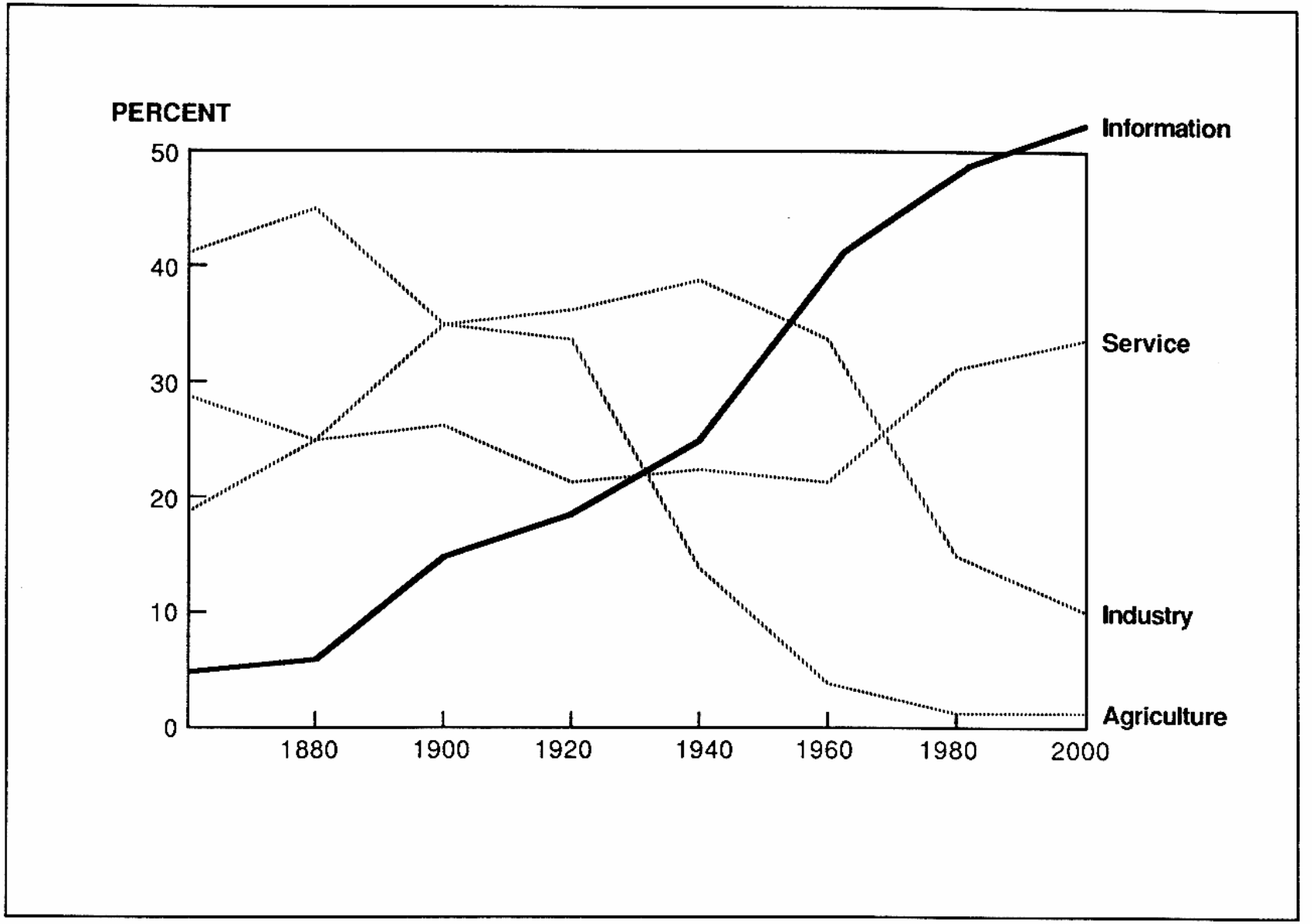

Figure 14. The Information Economy Distribution of the U.S. Workforce

1027); the endorser has been always NSA. Now there is DES being produced and sold that's not endorsed, because it couldn't pass the endorsement standard or didn't try. There is also some that is endorsed. You, the customer, decide what you want to do.

Oettinger: A very significant thing that you're witnessing here this afternoon is the emergence of this stuff into being like other measures for securing against a calamity, such as fire or theft, where there are gradations of security and a role for both government and nongovernment action. It is becoming a much more normal kind of thing as contrasted to its earlier status.

Daniels: Today when you have a secure phone, your regular phone and your secure phone sit beside each other; behind my desk there's five of those things, all different kinds. With the new ones coming out, you pull out your regular phone and you put in the new one, and you can still make all your nonsecure phone calls the way you want to; you make your secure phone calls by just pushing a button. So you don't need multiple phones anymore.

McLaughlin: If you're IBM and you want to buy a Hitachi phone ....

Daniels: If you're anybody. We were talking about losing them a little while ago. If I'm government X and you're government Y and I get hold of your crypto devices, I would think long and hard before I'd use one of them to protect my own stuff, because I know you built it. You probably know more about it than I do.

Student: Then it becomes a question of trade-off. If I don't have enough resources in order to invent mine, I may take the risk.

Daniels: Actually, technology is allowing me to protect against reverse engineering somewhat today and much better in the future.

Student: So, even if it's taken it's not necessarily compromised.

Student: Some people say it's no more than psychological warfare with the USSR.

Daniels: Well, I won't comment on that.

Student: I take it that NSA and other government agencies played a primary role in communications security and cryptographic technology, but probably much of that has now diffused out to the private sector. Would it be fair to say you're losing your dominance?

Daniels: No, I don't think so. There was a time when the private sector had locked onto this as being an interesting thing to work on. I have noticed that interest has dwindled way down.

Student: Why is that?

Daniels: I don't think they made any money.

Oettinger: This goes back to the fact that without government incentive or endorsement, there isn't a big market out there.

Student: But you're in the process of promoting a mass market with that CCEP approach.

Oettinger: The private sector may or may not respond. Jelen's piece* has some of the history of private/public relations; they've ebbed and flowed, as you'd expect, depending on who had the initiative. In the 1920s there was a period where the government didn't give a damn about this and the private sector developers were in fact interested. So the market reaction remains something to be seen.

*George F. Jelen, *Information Security: An Elusive Goal*. Cambridge, MA: Program on Information Resources Policy, Harvard University. 1985.