TRUSTED INFORMATION SYSTEMS, INC.
Computer Networking, Computer Security, Information Systems, Telecommunications

STEPHEN T. WALKER
PRESIDENT

September 26, 1983

Honorable Dan Glickman
Chairman
Subcommittee on Transportation, Aviation and Materials
House Committee on Science and Technology
United States House of Representatives
Suite 2321
Rayburn House Office Building
Washington D.C. 20510

Dear Chairman Glickman:

I appreciate the opportunity to appear before this Subcommittee on the subject of "Telecommunications Security and Privacy". My objective today is to point out the serious nature of the problems we face in this area, to describe some of the things which are underway now to deal with these problems and to discuss additional areas where work is needed in the near future.

Let me begin by describing who I am and why I believe this subject is particularly important at this time. I am President of Trusted Information Systems Inc., a small business which I recently founded. As the name implies, this business is concerned with development and use of computer systems which provide users with a high degree of confidence that their information stored in computers is protected from unauthorized use or disclosure; in short computers that users can "trust".

Prior to founding this company, I was the Director of Information Systems in the Office of the Deputy UnderSecretary of Defense for Communications, Command, Control and Intelligence at the Pentagon. In this capacity I was responsible for the World Wide Military Command and Control System (WWMCCS) Information System (WIS) and the Defense Communications System. I was also responsible for many of the advances in computer security within the Department of Defense (DoD) in the past decade. I spent four years at the Defense Advanced Research Projects Agency sponsoring computer security research activities. In 1978 I established the DoD Computer Security Initiative to 1) coordinate DoD computer security research activities, 2) encourage the development of trusted computer systems by the computer manufacturers, and 3) establish a trusted computer system evaluation process to determine the quality of industry and government developed computer systems. In 1981, following extensive negotiations with officials in the DoD and various other government agencies, the DoD Computer Security Evaluation Center was established at the National Security Agency to carry on the efforts of the Computer Security Initiative.

With this as background, I am pleased to give you my opinions on the topics which you have posed for this hearing.

The first topic you asked to be discussed is: "current and future threats and vulnerabilities to our information/communication technology dependent society."

The highly popular movie "War Games" should be required viewing for all who are concerned with protecting sensitive information on computers. Let me state emphatically that the national security related aspects of the movie are nothing more than very interesting fantasy, similar to that portrayed in dozens of similar movies and books in recent years. U. S. Military data communications systems are protected with the best communications security mechanisms and procedures available in the world, and computers are always used in advisory roles with humans making all the essential decisions regarding use of military force.

However, this movie is much more than just another interesting tale of Armageddon because the measures that the young high school student takes to gain access to his school's computer, the phone number of the airline reservations service and the bank's computer are all very real and easy to perform using small personal computers. The idea of programming a computer to run through all the phone numbers in a given phone exchange and note the ones that return a "data" tone is neither new nor in the slightest way sophisticated. Once one has a target phone number, the intuitive process for guessing the password of a user (assuming the system even bothers with passwords) is very well portrayed in the movie. It is these more or less routine aspects of the movie that users of computer systems should concentrate on because they represent the potential serious threats that users face.

The notoriety that the "414s" group in Milwaukee received in the past few months is not because they did something new or unique, but because they overdid it, attempting to break into over 60 business and government computers, according to Newsweek, and they got caught. What they did requires a modest amount of computer equipment, access to a telephone, a little bit of knowledge about computers (but really very little to start with) and a lot of spare time. All of these ingredients are abundantly available to thousands of potential "computer hackers" today. We can expect to hear about many more "414s" in the coming months and years!

But our vulnerabilities in this field are not limited to hackers. The wide spread connection of major information processing facilities by communication networks is inevitable with our ever growing needs for rapid communication. This growth in all areas of the commercial and government marketplace, from the major financial institutions to the local grocery store, offers inviting targets, not just for computer hackers to experiment with, but for serious fraud and illegal manipulations. Many local systems that were reasonably protected as isolated computers become easy targets for exploitation when connected to a major network. As the hackers have shown, the technical capability to penetrate these systems exists. Some recent activities have indicated that the intent to do "malicious hacking" also exists.

We need these highly sophisticated automated capabilities to carry on the functions of business as we now know it. How many businesses could afford to operate without computers today? And we want ever expanding facilities to allow more rapid response, better control and other related capabilities. Some managers will proceed with rapid automation without consideration of the computer security vulnerabilities and thereby risk their company's future. Other managers, fearing the potential damage that malicious hackers might do, may decide to keep their most sensitive information off the advanced automated systems, restricting it to local, isolated processing systems. Such a development could have an equally damaging effect, resulting a serious loss in business effectiveness. Many of the most serious problems encountered in the computer security area are directly traced to lack of understanding by management. Even routine security measures are ignored because security does not contribute directly to the "bottom line" of profits.

There are many aspects to the computer and communications security problem. There are a significant number of routine physical and administrative measures that should be taken to protect information on computers as well as the computers themselves. If particularly important or sensitive information is on a computer, care should be taken to know who has access to the computer just as one restricts access to one's personal files. Many of these simple measures are overlooked by owners and users of computers either because they do not understand the vulnerabilities or because they don't care about them.

Many people say that until users become aware of and put into practice these relatively simple and common sense local practices, they will have no need for sophisticated trusted systems. While I agree that it is foolish to operate a computer containing sensitive information without reasonable physical and administrative security procedures, the example of the 414s points up the additional major problem which confronts us. Whether a system has good physical security measures or not doesn't really matter when an intruder using a phone thousands of miles away can guess a password, or tamper with the login security measures. Good physical and administrative procedures (including proper password controls) are important but no longer enough in themselves.

There is a growing tendency to use add-on security packages to attempt to enhance the integrity of existing systems. If these systems, with their limitations, are fully understood and carefully employed, they can contribute a degree of protection that is not available in present day commercial systems. Unfortunately as the extensive history of system penetration efforts over the past decade has shown, if these add-ons are blindly applied and relied on for full protection, they can be easily circumvented.

What can be done about this problem? Your next two topics deal with this issue: "the scope of telecommunications security research efforts; and the extent of Federal and private sector efforts in improving computer security". Following my four years of sponsoring research in trusted computer systems at DARPA, I was convinced that in order to make real progress, the computer manufacturers must get deeply involved. The steps needed to build a trusted system start with the very innermost functions of a computer operating system and its hardware support. Unless and until the computer manufacturers understand and begin to utilize and improve upon the technical solutions presently known, further government research would only produce additional testbed demonstration systems. Government funded research pointed out several viable approaches to building trusted systems; now we needed to leverage that research by reaching out to the development and engineering centers of the manufacturers to get them involved. This was the major focus of the DoD Computer Security Initiative from 1978 until 1981 and it has had considerable success. Several manufacturers now have significant efforts aimed at building high integrity trusted systems and more are getting involved daily. These systems are not easy to build, requiring several years to evolve into useful systems but once available they promise to provide facilities that are resistant to hackers, malicious or not.

With this shift of focus to the manufacturers for the basic operating system tools, the DoD research goals shifted to understanding applications of trusted computer systems for message handling and data base management systems for example. Other parts of the Federal government have conducted activities in computer security for many years. The Institute for Computer Science and Technology (ICST) at the National Bureau of Standards (NBS) has done a good job of quantifying the overall nature of computer security vulnerabilities and has promulgated standards such as the Data Encryption Standard (DES), a very useful capability for providing protection to computer communication systems. The Department of Energy has also done considerable work in this field in recent years.

Your fourth topic points up yet another interesting situation in this complex area: "the scope of related legal, social and economic factors affecting telecommunications security". Here we encounter another dilemma. The computer manufacturers claim that they cannot spend the extensive resources to develop trusted systems until there is a strong user demand. The DoD requirements are discounted because they represent only a small segment (5% or less) of the market and no manufacturer can develop a general purpose system for such a small market segment. The user community on the other hand, often ignorant of the vulnerabilities they face as well as the potential solutions, will not demand this capability until they are sure that the solution is in place. Any bank that admits it has a computer security vulnerability without having a solution immediately available, is inviting its customers to take their business elsewhere. Since the banks and other users will not admit to having a problem, we come back full circle to the manufacturers.

Fortunately there is a way out of this "chicken and egg" situation. As I mentioned several of the manufacturers have proceeded with efforts to develop trusted systems, anticipating the need. In the next few years as recognizably better systems become commercially available, the banks and insurance companies will be able to put in place a better system, offering "state of the art" protection to their customers and creating a rapidly growing requirement for such systems. Recent efforts by the Securities and Exchange Commission to require that companies give assurance to their stockholders that they are doing everything possible to protect the assets of the company will have a very positive impact on the marketplace for trusted computer systems once they become generally available.

Your final topic, "the appropriate role for Federal agencies" in this field, is a very difficult one. There are two major categories to be considered: the role within the Federal government itself and the role for the private sector. Within the Federal government there is much to be done. The DoD now has a reasonable capability; the CSEC will provide the center of excellence in the evaluation of industry and DoD computer systems. The results of these efforts will spill over into the rest of the government and the private sector as the generalized evaluation results of systems become known. But care must be exercised here! The DoD CSEC cannot and must not assume the role of giving advice to the other Departments of the Federal government. Situated as it is in the Intelligence Community such a role would be, I believe, most inappropriate. Prior to founding the Center at NSA, consideration was given to forming a Federal Computer Security Evaluation Center, located at NBS and jointly administered by the DoD and the Department of Commerce. However, considerable resistance to such a facility arose within the DoD and there was little support for the idea from other elements of the government. It was recognized at the time of the decision to locate the DoD center at NSA that this would have a limiting effect on the applicability of its results to the rest of the government. The value of locating the DoD center at NSA outweighed this potential future problem.

Some means must be found for offering direct support to the other major elements of the Federal government because the computer security aspects of the Social Security, IRS and similar activities are very serious. Establishment of a Federal Center, working closely with the DoD Center is a possibility and NBS remains one of the few logical choices for such a facility. But it will be essential (and very difficult) to ensure that the two organizations do not overlap, or worse, contradict each other. This will be a difficult situation to resolve.

As far as the Federal government's role for the private sector, I believe that the government should limit its efforts to a major education and awareness program concerning the computer security vulnerabilities and available solutions. Such an effort coupled with the evolution of market forces should be sufficient to advance the state of the art for at least the next few years.

I indicated when I began that 1. the problem was real, 2. considerable effort was already underway and 3. there are still many things to do. I would like to summarize some of the remaining actions in concluding my remarks. First and perhaps foremost is the need for the strong education and consciousness raising program that I just mentioned. Perhaps we should thank the "414s" for bringing this problem into general focus in a relatively benign way, though we must be careful not to dismiss the general problem as merely the work of some cranks. As people become aware of both the seriousness of the problem and the fact that solutions are possible, I believe the normal forces of the marketplace will cause corrections to come into place. But without a serious education effort, this process will take a long time. I believe that hearings such as these serve a very useful role in this context.

There are difficult problems in this area that can only be resolved successfully by the Congress. One of the more difficult ones effecting the private sector and non-national security portions of the Federal government is the problem of personnel security. How can one learn enough about the background of a person about to be entrusted with sensitive corporate information without violating that individual's privacy rights? The national security community has long had a classification system for labeling degrees of sensitive information and a clearance system for assessing the trustworthiness of its personnel. The rest of the government and the private sector have neither capability and as a result have serious difficulty resolving rather fundamental security protection mechanisms. This is a difficult problem for which Congressional resolution may be required.

As mentioned above there is a need for a capability to work directly with the major civilian government and private sector users of sensitive information systems. How such a capability can be established and its relationship with the DoD are difficult remaining questions.

There is a need for more research into all aspects of the computer security problem. There is a tendency to focus on the high technology issues and disregard the more mundane requirements such as improved physical and administrative measures. There is also a need to find the proper place for such research outside of the DoD and to provide consistent long term support for such activities.

I could go on at much greater length on some aspects of this very important field but I hope my remarks here will serve as at least a partial summary of where things are today and where we need to go from here. Again, I thank you for the opportunity to express my views.

Sincerely,

Steph T. Walk

Stephen T. Walker