1 OCTOBER 2020

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 60495C
24 September 2020

MR JOHN L YOUNG
251 WEST 89TH STREET, #6E
NEW YORK NY 10024-1739

Dear John Young:

This further responds to your Freedom of Information Act (FOIA) request of 3 January 2010 for the following documents (cited in the footnotes of NDS DOCID 3417193 provided to you in FOIA Case 60251):

1. Unknown author, Fifty Years of Mathematical Cryptanalysis (Fort Meade), Md. NSA, 1988.
2. DDIR files, 96026, Box 4, Drake Notebook, Proto Paper.
3. Ibid, Unknown Author, draft history of COMPUSEC, in CCH files.
4. Interview, Norman Boardman, by Robert D. Farley, 1986, OH 3-86, NSA.

A copy of your request is enclosed. We have already provided you with Item 1 ("Fifty Years of Mathematical Cryptanalysis") and Item 2 ("DDIR files, 96026, Box 4, Drake Notebook, Proto Paper"). The final two documents, Items 3 and 4, are enclosed. Certain information, however, has been deleted from the enclosure.

Some of the withheld information has been found to be currently and properly classified in accordance with Executive Order 13526. The information meets the criteria for classification as set forth in Subparagraph C of Section 1.4 and remains classified TOP SECRET as provided in Section 1.2 of Executive Order 13526. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)). The information is exempt from automatic declassification in accordance with Section 3.3(b)(3) of E.O. 13526.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in this document. Accordingly, those portions are exempt

From: webteam@nsa.gov
Sent: Sunday, January 03, 2010 9:47 AM
To: FOIANET
Cc: jya@pipeline.com
Subject: Young, John - FOIA Request (Web form submission)

Name: John L Young

Email: jya@pipeline.com

Company: Cryptome.org

Postal Address: 251 West 89th Street, 6E

Postal City: New York

Postal State-prov: NY

Zip Code: 10024-1739

Country: United States of America

Home Phone: 212-873-8700

Work Phone: 212-873-8700

Records Requested:
Documents cited in notes of NDS DOCID: 3417193 recently provided to me by NSA:

1. Unknown Author, Fifty Years of Mathematical Cryptanalysis (Fort Meade), Md. NSA, 1988.

2. DDIR files, 96026, Box 4, Drake Notebook, Proto Paper.

3. Ibid, Unknown Author, draft history of COMPUSEC, in CCH files.

4. Interview, Norman Boardman, by Robert D. Farley, 1986, OH 3-86, NSA.

Thank you very much,

John Young

NSA - History of Computer Security

[redacted]

Manuscript

(b)(3)-P.L. 86-36

11 February 1998

CAUTION original document contains no classification markings except for chapter 6 which has a classification of ~~SECRET~~. Treat as ~~TSC//SI~~ until reviewed and appropriate classification is determined.

INTRODUCTION

Until 1965, the security doctrine of the United States was adequate for the protection of classified information in document and computer form. The doctrine was based on individual accountability for the documents entrusted to the person. Now, since the security doctrine was based on accounting for individual items (i.e. documents, papers, magnetic tapes, etc.) that stand in one to one correspondence with the information they contain, it was fairly easy to extend the principles to treat computerized processing of classified information. This extension was facilitated by the way in which computers were used; sequential, batch processing by single discrete programs that manipulated files of information stored on a single medium (e.g. tapes or a deck of cards). The key factor that permitted extension of the document handling security concepts to computer operations was the fact that the machines were oriented to serving a single user at a time. As a result, it was possible to isolate individual operations and apply security measures commensurate with the classification of the data processed. Additionally, the sequential servicing of individual users furthered the practice of user accountability for individual files, documents, storage media by permitting files to be recorded on separate storage media and only brought together for a given computer process.

By the mid-1960's, the research in resource sharing computer systems, conducted in many universities, had reached a stage of development that permitted a number of manufacturers to offer as a product resource sharing systems.

A resource sharing computer system is one that supports mutiple simultaneous use of the system through the technique of multiprogramming. The resources that are shared include primary and secondary storage, the channels and the central processor or processors of the system. The term resource sharing includes the types of operations known as 'multiprogrammed batch', 'remote batch', 'time-sharing' and 'interactive'. Where more than one processor is present in a system, with fully shared memory, the term also implies 'mutiprocessing'.

The nature of resource sharing, providing for two or more programs to be resident simultaneously in primary storage, eroded the separation principle that had been the underlying security practice. The machines also replaced the manual easily visible controls with reliance on logical and intangible program controls to keep separate the data and programs of different security classifications.

At first blush, the problems of providing security in time-shared systems seemed simple. One merely had to prevent any user from interfering with the operation of another and security was assured. This appeared obvious because the functional requirement of the operating system for time shared systems was to

provide for the integrity of mutiple programs active within the system. Unfortunately, this was not the case! The problem of providing security to time-shared systems was very complex.

The question of security control in resource sharing systems was brought into focus for the intelligence community, the Department of Defense and particularly the National Security Agency by a series of events in the spring and summer of 1965. By 1967, time-sharing systems were being procured in increasing numbers for government installations. Security of those systems became a pressing concern for the defense contractor and military operations. As a result, the System Development Corporation (SDC), a defense contractor, forwarded a position paper through the [redacted] to the Director for Security Policy in the Office of Assistant Secretary of Defense (Administration) soliciting action. Since the action involved technical issues, the paper was referred to the Office of the Director of Defense Research and Engineering for consideration.

(b) (1)
OGA

In June 1967, the Deputy Director (Administration, Evaluation and Management) requested the Director of the Advanced Research Projects Agency (ARPA) to form a task force to study and recommend hardware and software safeguards which would satisfactorily protect classified information in multiaccess, resource sharing computer systems.

What generated all this activity was an invitation and that is where our story begins.

CHAPTER 1

THE INVITATION

The System Development Corporation (SDC) of Santa Monica, California, expert in computer science and network communications, invited the Security Administrators from the Defense Department to a conference to be held on June 17, 1965. The conference was promulgated by concerns for unique security problems arising within the company, for the advent of computer technology was beginning to engulf classified information. SDC realized that the problems were about to impinge upon their defense contracts. The conference objective was to focus on the emergence of the problems in the handling of classified information within a computer.

Thus, began another chapter in the annals of computer science, later to be known as computer security (compusec).

The agenda centered on issues of computing, ranging from the security of time sharing to the protection of computer storage media. Participants in the conference were invited at the bequest of SDC in behalf of the company Research Security Administrators. The conference was structured around three agenda items: 1) Defining the problem, 2) Erasing magnetic storage media and 3) Electromagnetic radiation.

CONFERENCE AGENDA 1 - DEFINING THE PROBLEM

Dr. Donald L. Drukey, Manager, Research and Technology Division, SDC delivered the welcome address. He set the stage for the issues of the day when he addressed the audience with these remarks:

"...a computer being operated in a time-shared mode raises a number of problems in security and need-to-know control. We also have the added problem of compartmentalizing the information for use. We need guidance from the security community that will tell us what it is that we of the technical community have to do to convince you that you ought to perhaps grant a clearance to a computer..." [1]

---

[1]Robert L. Dennis, Security in the Computer Environment, (a professional paper, System Development Corporation, Santa Monica, California, August 18, 1966), 3.

The Security Officers probably answered the above quizzical statement with an emphatic YES. With that response begging the question; ok, where do we go from here? No one had the foggiest idea; Security Officers were not versed in computers much less aware of their vulnerabilities. So began a learning, exploring, research, groping period in securing computer technology.

The "technical" 1965 solution to the problems was to grant security clearances for all personnel who access the computer system. Their security clearances were granted to the highest level of the classified information processed by the system. Yet, even under this solution the need-to-know requirement was forgotten or ignored. As systems grew in size the problems compounded to the point of intolerance. Seeking solutions to the problems of a time-shared enviornment, ensuring the security of information stored on and erased from magnetic media and securing the electronic radiation emanating from a computer processing classified information were all problems that required attention. The basic objectives were to describe the problems and to make the Security Officers aware of the necessity to resolve them.

The Security Officers were presented with a case study. At SDC there was a time-sharing system allowing many people the use of one computer system, simultaneously. The SDC system had 53 users authorized; however, the average user population at one time on the system was 15 to 20. The user programs required storage because their were more of them than the machine could handle with only one auxiliary memory unit. The IBM Q-32 with its magnetic core storage required a second computer to handle the teletype messages and the two different computers required a buffer so they could talk to each other. This arrangement satisfied the storage requirements; however, anyone who knew how to use the system could call and use the computer along with the in-house users, thus potentially making one user's data accessable to another user. In a time-shared computer system, a number of users were operating simultaneously, each with an independent program. That is, each program had a series of commands, instructions and data that were resident in the processor. Therefore, accidentally or deliberately, a user is able to obtain access to another user's data and thus commit a breach of security. For in a time-sharing system, there are many places where the data from one program were mixed with the data from another program. Although, the user always knew the location of the data; the problem was how to keep other users from getting that data. The obvious solution to this problem is to prevent unauthorized access. The real trick is how to implement this barrier with 100% effectiveness. Almost any control could be defeated from the maintenance console!

Another inherent vulnerability in time-sharing systems was the commmunications topography. For example, security cleared users were within the same general area as the computer and had direct connect to the computer. This allowed the computer to easily

distinguish the channel to which that device was attached. It then could provide identification of anyone who had access to a particular device and constrain access to those programs associated with the particular channel. However, it became a different problem when the users were at a remote device connected to the computer through the switching facilities of the telephone company. Line tapping was a possibility and it necessitated some other means of user identification. Another situation in which the lines were secure but the device was not, would prompt the establishment of some kind of password arrangement.

The problem to solve was how to block the unauthorized user from gaining access to classified data. A solution offered at the conference was to take advantage of the memory protection feature that was employed by small and large manufacturers. This feature was designed as a basic control function for protection of data. Consider the following case in point. Many programs and particularly new programs were fraught with programmer errors. If one or more of these errors were able to jump (and it could) into another area occupied by another program, it would contaminate the other program. Further, suppose the jump occurred into the area where the executive (operating system software) program was resident, then all on the computer were in trouble. Without orderly control and scheduling of programs, the computer could not perform the functions for which it was designed. Memory protection was of necessity required!

The schema of the memory protection feature can be explained in the following manner. Consider computer memory as a long list of defined spaces. A programmer was assigned a defined block of spaces within this long list. Every time the programmer filled an assigned space the computer assigned a unique address to that space. Each time the program performed some instruction the computer would compare it with the boundary address within which the program was assigned and must reside. If it stayed within this boundary, fine and well; however, if the program attempted to execute an instruction outside the boundary then the program was halted! In the language of the diagnostics from the computer, the programmer would then receive a message something like "program exceeds memory bounds".

The question was, how good were the protection schemes? Robert F. VonBuelow, Head, Laboratory Development and Operations Staff, Technology Directorate, SDC, suggested that for every new computer and system a trial of test and evaulation be conducted by someone who was intimately knowledgable of the computer system.

The practice of the day was to keep secret the discovered tricks that violated the memory protection scheme. The reason for the secrecy was to safeguard some other system that was not protected.

VonBuelow called for a change in the way business was done! A call was echoed for some kind of an agency which gathered

together and disseminated to the people concerned all the ways a computer system could be violated. It was here that the beginning of formalized computer security was recognized and the seeds were planted for the establishment of a computer security authority in the Federal Government. As we shall see, the germination of this seed experienced difficulty in establishing root and then bearing fruit. However, for now, let's return to the conference and learn what other problems were discovered and presented to the security officers!

When SDC took delivery of their IBM Q-32 computer, it did not have memory protection, it did not operate in a time-sharing mode, but operated in a serial batch processing mode. SDC personnel decided to build a memory protection mechanism and it was perceived to be adequate. However, when placed in operation, numerous ways were discovered to defeat it. The defeats came at the request of SDC by placing one of their knowledgable personnel on the system with the instructions to attempt to defeat the memory protection feature. The employee discovered more than a dozen different ways to by-pass the feature. As a result, SDC took preventive measures both in hardware and software to positively prevent further violations. SDC reported that, to the best of their knowledge, no new memory protection violations had occurred. The techniques were offered as a contribution to a future body of knowledge to be administered by a central authority.

CONFERENCE AGENDA 2 - ERASING MAGNETIC STORAGE

Dr. Willis H. Ware, Head, Computer Sciences Department, Rand Corporation, was invited by SDC to be a speaker at the conference. He introduced the audience to the problem of securely erasing magnetic storage media.

The session was concerned with information recorded on storage devices, be it core memory, tape, drum or disc. In order for a computer to be successful, it has to be designed so that any information written onto a storage device can be overwritten or, as was more popularly stated, erased. For the user, the act of overwriting was considered synonymous with erasure of information. Summarizing one element of the security problem that was previously touched upon was the unauthorized reading of information from any magnetic storage device that was actively connected to the machine. This could simply be performed by the program executing a read of the assigned storage areas prior to any instruction to write in those areas. This was a big problem with time-shared systems. A programmer could, accidentally or deliberately, gain access to another programmer's information whether it was in core memory or on tape, drum or disc. All storage media were subject to the same problem. The safeguards against unauthorized access were in hardware and software. Willis Ware believed that neither alone was sufficient. He pointed out, in extreme cases, that one would

probably encrypt the information prior to introducing it into the machine.

The question was asked; can classified information which had been written on one of the magnetic storage medium be destroyed in the security sense without physically destroying the medium?

Traditionally, security professionals usually thought of declassification as total destruction. Burn or mulch paper, melt film and destroy devices. No effort was made to destroy the information without destroying the medium on which the information was recorded.

Security was trying to deal with computer information in the traditional manner. Destruction of the computer storage medium was not an economical one. It was paramount that new ways be found to destroy the information without destroying the storage medium. The design of the computer system was such that the most recently recorded information was read. The computer is unable to read previously recorded information that it has overwritten. The problem of declassification of the medium was solved by overwriting, provided the computer can, in fact, overwrite the magnetic surfaces completely. Because the computer read only the most recent information, it appeared logical and sufficient to overwrite the classified information with nonsense information. Security personnel would require that the writing did in fact occur and that it occurred over every location of the magnetic storage medium.

At that time, such procedures were in practice. Air Force regulation 205-1 specified that streams of random digits written over classified information at least three times was sufficient to declassify the media. The reason for multiple writing was to make certain that all classified areas have been overwritten. There were hardware and software anomalies that could occur and thus negate the intent of the overwrite procedure. So, to avoid such failures, the regulation required repeated writings at least three times. This procedure certainly worked for magnetic drums; the question was, would it work for tapes?

The tape problem was different because they were removable. A reel of tape could be removed from the machine and subjected to tampering. A disc pak was also removable and subject to similar tampering. The ease of removing the tape was as simple as taking the tape off a " hi-fi" tape transport. The disc packs were removed from the machine exactly as you would remove a stack of records off a turntable. The overwrite procedures, as far as the machine was concerned, could guarantee that past history was not accessible to the computer.

However, the removable media, tape and disc, were susceptible to unauthorized possession. Consequently, this media could be subjected to some special laboratory technique wherein one might be able to discover the past history of data recorded

thereon. Ware mentioned that he understood that such experiments had been performed to recover overwritten information. Certainly, the Air Force regulation acknowledged the possibility of recovery of latent information; and, it specified that tapes once classified must remain so. This regulation only addressed the tape, but not the disc, recoverability.

From this discussion, it was clear that experimental work was needed to discover the severity of the problem and to find solutions that dealt with it.

Additionally, there was a related problem; what happened when you returned a system to the manufacture or transferred it to another installation with a different or no security status?

All of this pointed up to the fact that very little guidance was available to industry as to the disposition of classified information contained on magnetic storage media in computer systems. The incentive to solve the problem was economic.

[redacted] for all Defense contractors, covered no aspect of the problem. And, while one military regulation dealt with one aspect of the problem it left much to be addressed.

(b) (1)
OGA

Ware believed that many of the problems were technical in nature and could be resolved with very little difficulty. He felt that given sufficient resources, of engineers and computer programmers, the problems could be resolved within a year! He believed that there were overwhelming political and administrative problems in the establishment of a focal agency; and this he viewed as the real problem. However, he believed that an established central technical authority was paramount to solving the problems. He even outlined the role of the central agency to encompass the following responsibilities. The agency would be authorized to conduct tests and establish standards. Further, it would determine policy and have the authority to promulgate and enforce that policy upon the military and industrial users responsible for processing the classified information in their computers.

CONFERENCE AGENDA 3 - ELECTROMAGNETIC RADIATION

Jerome A. Russell, Computation Division, University of California, Lawrence Livermore Laboratory, opened this session with the following remarks;

"I am here to talk about electromagnetic radiation, and this we all have. Each machine radiates electromagnetic energy because of the wires transmitting current, and magnetic and electrostatic fields are generated by these--they are all actually little transmitters. The entire machine sends out radiation. Every

time a magnetic tape transport starts and stops, you get wide bands of transmitted noise.

Our problem is to minimize the possibility of someone outside the fence picking up these noises, and they can be picked up if you have a sophisticated enough reciever."[1]

Russell went on to explain and describe the preventive measures that Lawrence Livermore employed for radiation protection. A great deal of effort was expended at the Labs to safeguard from electromagnetic radiation leakage. For example, the Edison Company lines entering the buildings were all run through shielded banks. This configuration also prevented the information from going back to the power lines and thus protected the computers from radiation.

The teletype terminals were interfaced to a multi-programming and multiprocessing system named "Octopus". The cables of the terminals were shielded according to a classified regulation which prescribed a shield of a certain composition. There was no sharing of the telephone facility with regular voice line systems.

Following the discussion on Electromagnetic Radiation, Russell highlighted additional problems that confronted their operations. They were concerned about their systems' lack of ability to generate a classification at the top and bottom of each printed page.

Also, the Octopus system was unable to account for or record events that preceded a system failure. Audit trials were non-existent. The system was described as experiencing a once in a while failure, and when that occurred it was very difficult to know what happened. The programs in process were ruined and they required re-initialization when the system was restored to normal operations. No diagnostics existed to audit these failure events! The lack of accountability not only impacted upon operations but also had a negative effect upon security requirements and responsibilities. Accountability of events is essential when security authorities are conducting a damage assessment of compromised classified information. Audit trails of a security nature were an essential element that required development.

Guidance was also being sought in the photograhic digital information handling process. The nature of this unique mass-storage system was described as follows; a piece of photographic film, 35mm, had data fields recorded on it in digital form. Each record contained thirty two of these small chips of film in a plastic box grouped with other boxes resident in large plastic trays. A number of these trays were moved back and forth mechanically and pneumatically. Here was an example of the technology of the day outmoding the security policy of the time! For, there were no regulations for holding documents of this kind!

---

[1]ibid.,16.

The security procedures for safeguarding magnetic storage media were sparse whereas the security procedures for safeguarding photographic digital information storage were non-existent.

The Octopus system programmers took some measures to insure integrity of the data. Complete records were maintained of request of individuals not normally granted general access to specific areas of the system. The motive for this structure design was not for security but for the protection of another individual's information from being wiped out. It turned out that this type of partitioning structure had value in security practice. However, a weakness in the structure was that the individual was not positively identified and sanctioned by Octopus. If the individual was communicating from an authorized terminal and knew the correct entry words to a restricted area of the computer, the individual was granted access! Positive identification of the user was needed.

With the conclusion of the session on Electromagnetic Radiation, the conference ended its' formal presentations of the problems.

Obviously, more questions were raised than solutions offered. The participants conversed about the problems that were presented and all agreed that an extensive amount of work was needed. For very few, if any, adequate answers were forthcoming to resolve them.

In summary, the conference called for research into the vulnerabilities of computer systems. It included the investigation of the phenomena of magnetic properties of storage media. Solutions would be sought that would achieve the declassification of the media without destroying them. Individual computer hardware and operationally configured systems required evaluation of their electromagnetic radiation properties.

A central technical authority was desperately needed within the U. S. Government. It would act as a central clearinghouse for developments that transpired in the pursuit of computer security. The authority would also pass judgement on the security effectiveness of operational systems. The conference concluded on a note of confidence that further action would be forthcoming in addressing the issues of data processing.

CONTACT WITH NSA

No public discussion of the subject matter was pursued during the following year. Then on 18 August 1966, the published proceedings of the conference were available.

A few days later, on 26 August 1966, Lieutenant General Marshall S. Carter, Director, National Security Agency received a

letter from Willis Ware, in his role as a member of the Electronic Data Processing (EDP) panel of the Natioal Security Agency Scientific Advisory Board (NSASAB). He apprised Carter that the advent of shared computer systems raised serious questions with regard to security. In addition, he told him of a corresponding issue called the "privacy problem". This problem was not only developing in the industrial and commercial utilization of computer networks but was also occurring in that part of the U. S. Government that did not operate within the framework of classified information.

He informed the General of a very powerful movement in the computer industry toward so-called online, time shared systems. A time shared system was an idea that permitted many users access to a machine through individual remote terminals. This raised serious questions about the security and integrity of information within such computers. For, the industrial priority was first and foremost in the development of the technology and security of the data was a passing thought, at best! Ware believed that a new mission was on the horizon!

"I visualize that there may be a significant new role in the making for NSA, and that major new technical developments now maturing may lead the Agency into much broader missions."[1]

Ware's idea of a "much broader mission" not only involved the security of systems processing classified information but also included the "privacy problem". He maintained that there were many similarities between the two problems; for example a requirement to maintain the integrity of the data; need-to-know controls; and secure communications.

Ware raised a very sensitive issue when he portrayed the scenario that once commercial interest identified the computer security needs, there might emerge an independent, non-government counterpart to NSA. This thought struck at the very heart of the mission and many within the Agency feared such an event. Their belief was and still remains today that commercial applications of cryptographic principles applied in computer systems could do grave damage to the capability of the intelligence mission of NSA.

Ware concluded his correspondence with an offer to assist the General and NSA in any way he could.

ON THE POLITICAL FRONT

At about this time, in 1966, a Democratic Congressman from New Jersey, Cornelius Gallagher, chaired a special subcommittee of

---

[1]Willis Ware correspondence to DIRNSA, Gen. Carter, dated 23 August 1966, expressing concerns of security in computers.

the House of Representatives Government Operations on the invasion of privacy. The hearings were the first of their kind regarding computer technology and the need to establish ethical and legal protection as well as technological safeguards for certain computer applications. They would not be the last!

The purpose of the hearings were to establish a "climate of concern" in regard to the Bureau of the Budget proposal for establishment of a data bank. The bank would combine all personnel and business files that were maintained by different government agencies. Motive? Efficiency!

Gallagher was concerned that the consolidation of data could result in a breach of privacy protection with the potential for misuse of the information. Here were the elements to exercise power and control over individuals and business. For example, the FBI files also contained unsubstantiated gossip against many individuals; the IRS files contained detailed financial and business data; and the Civil Service Commission files covered a widely disparate range of information.

The subcommittee heard government spokesmen assure them that they were "men of good faith" and they would hold faith with the rights of the individual. How could the committee possibly not have faith in their expression of good faith? The subcommittee asked what informtion would be included in the proposed data bank? What protection of privacy would be built into the system? Who would have access to the information? No specific answers came forth! The subcommittee was not impressed.

Next, the members of the subcommittee listened to the views of the computer community as expressed by their representatives. Concern was voiced over what they perceived to be a natural and unavoidable trend toward multiplicity of data once a system was established. They testified that present hardware did not contain sufficient safeguards against unauthorized persons tapping into the files. The subcommittee agreed with the concerns of this group and recommended against any establishment of a universal data bank.

The Gallagher subcommittee goal of establishing a "climate of concern" was effective, at least at NSA. Mr. George Hicken, the Community On-Line Intelligence System (COINS) manager, expressed concern for the COINS network. He felt that this network concept under developement within the intelligence community would next be brought under examination by the subcommittee. The purpose of the network was to provide access to various data banks throughout the agencies of the intelligence community to an analyst querying the network from a single terminal. It was similar in concept to the Bureau of the Budget proposal. Hicken felt that since the basic idea was not acceptable, it could have far reaching effects even though the COINS concept was not a target of inquiry by the subcommittee. Conseguently, Hicken placed great emphasis on the development of computer security techniques for the network. He

even offered the COINS network as an experimental testbed. As it turned out no inquiry was made and the COINS network continued in its' development and contributed much to the development of computer security.

The hearings also precipitated a flood of adverse public articles against the idea of a universal government data bank. The theme of the articles centered on government as "Big Brother" and as such threatened the loss of individual rights. The stories were prevalent in the technical computer publications of the day. The subject even caught the attention of the popular press where similar articles appeared in publications like Newsweek and the Los Angeles Times.

In separate correspondence, Ware apprised NSA of this political and popular press activity. He felt that it was time for the NSASAB to give consideration to the computer security issues.

Dr. Louis W. Tordella, Deputy Director of NSA, assured Ware that the computer security issue merited consideration within the NSASAB structure. Also, the matter was disseminated to the NSA Assistant Directorates responsible for such matters. Tordella requested Ware to discuss the situation with his fellow members of the NSASAB EDP.

Ware followed-up on the Tordella request and on 27 December 1966 corresponded with the NSASAB secretary, Thomas A Prugh. He wrote that up to now, public discussion of the problem had been mostly about social, legal, political, moral and ethical issues. Therefore, he had made written recommendations to the Board for Computer Conferences, a group that organized and sponsored international semi-annual conferences, that the spring conference should have sessions on the technical aspects of the problem. The Board members were delighted with the idea and requested Ware to host a computer security segment of the conference in their upcoming spring conference to be held in Atlantic City, New Jersey during 18 - 20 April 1967. He maintained that he did not intend to be involved in the conference but was unexpectdly asked to chair and organize the session on computer security. He accepted the invitation and wished to assure the Agency that although some areas of this new field could touch on sensitive matters related to the NSA mission, he would keep the conference conversations from "wandering onto dangerous grounds".[1]

Thomas A. Prugh expressed concern that this activity of Wares' was unconsciously leading the Agency into a role it may not be prepared to cope with. Prugh planned to relate his concerns to Ware during a meeting of 20 January 1967.

---

[1]Dr. Willis Ware correspondence to the NSASAB secretary dated 27 December 1966, concerning his chairing a public session on computer security in Atlantic City, New Jersey during 18-20 April 1967.

OPERATIONAL PROBLEMS CONFRONT THE NSA

On 26 January 1967 [redacted] Virginia. The agenda was concerned with the actions taken as a result of the SDC conference. In addition, [redacted] to present current operational problems that requirted solutions. In attendence were members from System Development Corporation; Bell Telephone Laboratories; Lawrence Livermore Laboratories; National Security Agency; Advanced Research Project Agency; and Defense Supply Agency.

The meeting opened with [redacted] reviewing the events that had followed the conference. He provided the contractors with guidance on erasure procedures for magnetic media. [redacted] noted that the erasure procedures were incorporated [redacted] it was expected that of the 50,000 computers in the United States by 1970 over half would be used in time sharing. [redacted] the Federal Communications Commission (FCC) anticipated a large increase in the use of computer communications via telephone, telegraph and other common means of communications. There was a serious concern for the integrity of this data and security guidance was desperately needed.

(b) (1) OGA

The participants agreed that there were two serious problems associated with computers. The first problem was controlling access and the second was security of computer data transmission. The communications problem was directed toward the NSA representatives of the Communications Security organization, Mr. Jerry Friedman and Mr. Owen Crowder. They were asked if NSA would address the communications problems of computers.

Friedman responded to the issue of NSA involvement in computer security by explaining that the Agency only got involved when CRYPTOGRAPHIC equipment was associated with the computer system. Crowder added that NSA, by regulation, can not approach a contractor about a cryptographic system without the sponsoring Agency making a request to NSA. In turn, the sponsoring Agency passed the advice on to the contractor. There was no one-on-one exchange between the contractor and NSA.

Although the Friedman explanation was legally and jurisdictionally accurate as to the limited role assigned to NSA,

(b)(1) OGA

it was not well received! The NSA answer left the issue of current operational problems unanswered. [redacted] remarked that it was obvious that the Government needed to get its' act together. He said that it was the responsibility [redacted] for action and that he would do so. All agreed and the meeting adjourned.

Back at NSA, the comments of Friedman became the cause of some consternation within the COMSEC organization. The issue was a lack of NSA policy regarding computer security, particularly when cryptographic equipment was not involved. A policy statement was under review in the COMSEC organization and in other areas of the Agency. However until a policy was published, NSA would officially remain uncommitted.

Mr. David Boak, former Chief, Operations Division, COMSEC believed the remarks of Freidman to be completely accurate. It represented very clearly the present policy of the Agency. In fact, Boak believed that Friedman had performed a service for NSA by shielding the Agency from a deluge of inquiries it was neither charged nor equipped to handle.

(b)(3)-P.L. 86-36

Well, the flood gates were not to hold back the deluge for long, for leaks began to occur. [redacted] Friedman offered to assist the ARPA in their ADP security requirements. On another COMSEC front Crowder along with [redacted] affirmatively responded to a request from the National Aeronautics and Space Administration (NASA). This involved a visit to one of the NASA contractors. In the Pentagon, the design of a new world-wide computer network was underway. It was known as the World Wide Military Command and Control System (WWMCCS) and NSA was requested to assist in the formulation of its security parameters.

In California, NSA liaison officer John A. Planey was confronted with a computer security issue that necessitated guidance from NSA Headquarters. He brought to the attention of NSA an Ad Hoc committee report from the Stanford Research Institute (SRI) entitled "Problems in Security of Computer Systems" dated March 10, 1967. The report urged that the Secretary of Defense issue a directive that assigned responsibility to a Department agency. The authors of the report "especially" believed that the knowledge, interest and responsibilities of the National Security Agency made its active participation essential from the onset. The SRI intended to proceed on its own should NSA not take action; it would study the problem and identify solutions. Planey urged NSA to address the issue and establish policy. He was informed that NSA directorates aligned with computer science issues were giving further thought to the NSA policy issue. In the meantime, NSA would lend a sympathetic ear to the problems brought to its' doorstep.

In all of the requests received at NSA, the requestor was cautioned that NSA chose to assist in an unofficial capacity. NSA arrived at this posture due to the absence of any other

(b)(1)
OGA

knowledgeable body. They would continue to help in this fashion until an official designee was appointed.

On 16 March 1967, [redacted] attended a prearranged conference with the COMSEC representatives at NSA. [redacted]

[redacted]

At the conclusion of the meeting, the NSA members promised to pursue a change in the COMSEC doctrine, a change that would recognize the need for security in computer usage in the Defense and Industrial communities where cryptographic equipments were not used.

Chapter 2

(b) (1)
OGA

THE ROLE OF NSA IN COMPUTER SECURITY

The published proceedings of the June, 1965 conference at SDC in California; Dr. Wares' correspondence and discussion with NSASAB; the NASA request for security assistance; [redacted] the WWMMCCS request and many more calls for assistance prompted NSA to examine the role it should play in computer security. This examination began with a " think paper" prepared on 6 June 1967. The paper was written in S061, the technical staff of the Communications Security organization and it was coordinated by Jack W. August, a member of the staff.

In the paper the problem was addressed in a question format. To what extent, if any, should NSA become involved in computer security? How will the program be implemented? Will additional people and/or special training be required? Where do the people come from?

A lengthy discussion and debate of the issue was set in motion. It was recognized that ADP equipments utilized many of the electromechanical and electronic components found in other types of electronic equipment that store, process, transmit and manipulate information. Therefore, some existing COMSEC measures may apply to computers. However, the problem was compounded by the rapid pace of the evolution of the computer technology and along with the change came an explosion of operational use of the systems. This increased usage led to demands for interconnectivity of the systems, thus providing ever increasing access to an ever increasing number of files. The issue was how can NSA provide protection and security controlled access to this vast array of information.

The writers assumed that should the NSA accept the responsibilities, it would most certainly include the computers in operation throughout the Federal Government. A thought not far fetched given that this scenario was coming from an organizational group chartered with the responsibility to provide communications security for the Federal Government.

Also, if NSA became involved in the business of computer security the circumstances would be wide and varied. The new circumstances would, most certainly, be beyond the scope and experience of COMSEC functions. Could NSA perform competently in this new enviornment? A sample of the situations possible in the field that could be encountered were amplified for the benefit of the decision makers.

A computer in an unsecured or secure area processes small amounts of classified information and some of that information is

stored on drums or core memory within the system. There are no external transmissions except to input/output devices. The system is accessed by cleared and uncleared users. How is such a system secured?

A computer which has large amounts of classified information and can be interrogated from numerous local terminals within a building or complex. (RYE/TIPS system at NSA for example).

A computer which has large amounts of classified information and has lines to distant terminals which are protected by cryptographic equipment. (COINS for example).

A computer which is used as a message switch processing classified information exclusively (DIA switch in the COINS system).

The examples of real situations required decisions to be made and it was hoped that the decision process would aid in the formulation of Agency policy. Other questions addressed the physical security problems that accompanied the computer system.

Questions like, will NSA prescribe the physical security criteria for the area in which the computer is stored? Will NSA prescribe the physical security criteria for the area in which all outlying terminal devices are located; even if only unclassified information is being processed at the terminal but the computer has classified information within it? Will NSA prescribe the criteria for the protection of communication lines connected to the computer within the building complex or to a distant point?

Will NSA limit its responsibilities to "fixed plant" ADP or will such responsibilities also apply to mobile configurations or to ADP operated in a temporary location for short periods of time (less than 6 months)?

Will NSA prescribe TEMPEST requirements for the computer and for the input/output devices?

As to the question of compromising emanations, draft guidelines for the application of compromising emanations control and techniques to ADP facilities were being staffed. The guidelines indicated that ADP equipment runs the gamut of complexity. The authors annotated the draft to reflect their concerns about this complexity. They felt that it may be prudent to apply general TEMPEST protection features to the systems. This approach was in contrast to the specific applications protection that was based on test data obtained from individual equipment evaluations. The TEMPEST shielding of individual equipments could be expensive and very time consuming.

The TEMPEST draft guidelines were submitted to a United States Communications Security Board (USCSB) committee for comment. The responses varied from "nil" to complete disagreement. The CIA,

NSA, and Navy felt that some protection was necessary, the DOD DDR&E indicated that little or no protection was required. As a result of the comments, it appeared that the NSA COMSEC organization would have to come up with their "best estimate" of the threat, realizing what they proposed was challengeable. The end result was to be a publication of an "in-house" NSA quideline to be available if and when NSA was approached as to how to handle the TEMPEST problem.

The research organization of NSA, known as R&D, indicated that the Agency can safely assure all users of time-shared computer systems that the communications security aspects of such systems were adeguately covered under R&D programs.

However, SYSTEM security protection for time-shared computers had a very long way to go. The security of remotely accessed computer systems appeared to be a very large problem reaching well into the future. The NSA R&D organization had no plans to devote a large work effort to this problem; even an acceptable contractor had not been found to accomplish a modest study on the subject.

The "think paper" up to this point addressed the computer security problem as it related to national security. However, U. S. congressional hearings on the invasion of privacy (Hearings on the Computer and Invasion of Privacy, July 26-28, 1966) pointed out that in the name of scientific advancement the rights of the "individual" were being threatened by both private and government computers containing "privacy data". The hearings brought out the need for safeguards. Recommendations for the protection of the data entailed technologies directly related to the computer operations and the communications of the information. The hearings urged that minimal cryptographic protection be applied to all the communications lines. There should be better control of the programmers of computer systems. Random external audits of file operating programs were advocated to insure that a programmer did not intentionally or inadvertently create a "trap door" that allowed remote access to unauthorized information. Finally, mechanisms within the system should be available to detect abnormal information requests and identify such a requestor.

The congressional hearings recognized that industry and government faced similar problems in the esatblishment of computer security. Therefore, it appeared that early action was essential among interested activities to further define specific areas in which NSA would be responsible or at least provide guidance, standards, criteria or parameters. Additionally, simultaneous consideration should be given to identify those areas or specifics that should be addressed by other than NSA.

As regarding the manpower required for this effort, initial capability within the S organization could be developed around "very few people". One of two approaches were possible.

First, the establishment of a single activity within the S organization with primary responsibility in the computer security field.

The second approach entailed the formation of a panel, chaired by S1 and composed of individuals selected by the Chiefs in S1, S2 and S06. They would periodically meet at the call of the chairman. This latter approach was the recommended way to proceed because it would take immediate advantage of expertise available throughout the S organization.The assignment of 6 or 7 people to the panel would appear to be adequate, however the division chiefs would have the final word on the composition of the panel.

What was the impact of this course of action? The formation of an S computer security panel would give "immediate significant support" to the steadily increasing demand for clarification and/or resolution of decisions. Additionally, the panel would provide the mechanism and a single source of contact on computer security problems with NSA staff in R, P, C, etc. Finally, the panel would serve as the point of contact to determine the usefulness of the approach taken by industry to solutions of related computer security problems.

The "think paper" was prepared by the S06 organization inorder to serve as the focal point of discussion at a meeting on Computer Security attended by members of S111, S061, D42 and S06. The purpose of the meeting was to determine what should be done regarding the Staff Study on Computer Security; should NSA get involved; and, if so, to what extent?

Tom R. Chittenden, S organization, responded to the "think paper" with some ideas of his own. He expressed his thoughts in a memorandum of 7 June 1967, entitled SOME THOUGHTS ON THE NSA ROLE IN COMPUTER SECURITY.

Excerpts from the memoradum read as follows:

"... In this paper I have gathered together some ideas and suggestions for the eventual development of a clear-cut statement for presentation to the Director and possibly the USCSB on the role which we believe NSA should have in the Government in the field of security as applied to computer operation and intercomputer communication. Included in this field, which still has no adequate name, is the so-called privacy problem which covers the host of problems involved in maintaining the integrity and authenticity of information stored in or processed by a multi-access, time-shared computer system..."

"... I believe that the NSA role should be designed to shrink the actual NSA activity as other departments and agencies acquire knowledege and capability and the staff... In other words, we should start out broadly in order to fill the present vacuum and then diminish our direct involvement... In my view, NSA needs to have as its primary objective the decentralization of most of the

computer security activities... We should encourage agencies to acquire and train people competent to design, advise and evaluate computer security activities in their specific agency... ".

The agency charter (NSC 5711) revision was underway and a list of functions defining NSA involvement in computer security were included. This re-defining role of NSA to include computer security was heavily influenced by the Chittenden remarks. See Appendix B for the suggested revised COMSEC functions of NSA.

THE NSASAB GETS INVOLVED

On 27 June 1967, the National Security Agency Scientific Advisory Board, with member Dr. Willis Ware, advised the Director, Lt. General Marshall S. Carter, of the following computer security situation. The relative few time sharing systems that have been built incorporate certain information protecting features for the sake of the user. The NSA RYE system was the only one that incorporated broad protective features that guaranteed security of the information. At the moment, NSA was in the advantageous position of having "done the job" and hence, had experience and expertise not elsewhere available.

There was a highly variable degree of concern about the whole security and privacy issue. Those of the NSASAB who had been closest to the matter believed that the security problem, was very near and serious. Other views held that the problem was not nearly so imminent. Whichever the case, it was recognized that it would take time to straighten out the government regulations, and hence, the membership felt that now was the time to formulate technical solutions to the problems.

Further, the NSASAB advised Carter that the Federal Communications Commission (FCC) would shortly hold hearings which touch on the privacy problem. Collectively the membership stated,

"While we appreciate that NSA will not want to become embroiled in the political surroundings that will accompany these hearings, at the same time we wonder whether you might let it be known through channels that you can contribute expertise and technical guidance.

We framed some questions which we could not answer. I (Dr. Ware) record them here in case they might be of value in attacking the security question. Would a Presidential Executive Order be an appropriate vehicle with which to deal in computer security matters on an interim basis? Might it be possible to revitalize the USCSB and vest responsibility for computer security there? Can NSA play a role in the education of the defense community to technical aspects of computer security? The general government community? The industrial community? What is the proper role of NSA in the matter? Advisors? Trainers? Consultants? All?"[1] Carter considered the advice of his scientific advisors but chose to await the internal NSA staffing before arriving at a decision.

---

[1]National Security Agency Scientific Advisory Board (NSASAB) meeting minutes of 27 June 1967, L-12138, addressed to NSA Director, Lt. Gen. Marshall S. Carter

EVOLUTION TO THE "ROLE" PAPER

The "think paper" of 6 June 1967 was not a formally staffed document, however it did serve the purpose of generating a document that was formally staffed throughout the Agency; entitled, "The Role of NSA in Computer Security". It was prepared by the COMSEC organization on 23 August 1967. This paper was widely coordinated amongst Agency elements in production, research and development, communications security, policy and administration.

The reader was introduced to computer security by the concept of on-line, computer to computer communications and data processing as fact and no longer a theoretical concept. Two realities had been increasingly apparent to those involved in security: (1) There was an immediate and growing need for a source of guidance as to the means of securing computer communications and (2) The security of online data processing complexes may be separated from that of communication processors only with the greatest of difficulty. These were complimentary facets of the same capability -- high speed information exchange -- and omitting either from the blanket of security, negated whatever precautions had been taken to protect the other.

In the past year, the void in the area of computer security had become strikingly apparent. In August 1966, the System Development Corporation again hosted a seminar with the main objecvtive being "to describe our (contractor) problems and to make you (government representatives) aware of our need for extended quidance." From the proceedings of this seminar, it was apparent that commercial contractors in the computer field had the capability to incorporate many safeguards into original equipment designs and were cognizant, if not more cognizant than the government, of the need for guideposts in this area.

At the 1967 Spring Joint Computer conference, one of the best attended sessions was Security and Privacy in Computer Systems chaired by Ware. In the session, NSA Chief, RYE System, Mr. Bernard Peters presented a paper on the Security Considerations in a Multi-Programmed Computer System. This and other presentations evoked extensive audience interest and the need for direction in this area was very apparent.

Ware of the Rand Corporation had been one of the most vocal adherents of the need for computer security criteria. In his own words,

"the real problem is to establish some focal agency to conduct tests, to establish standards, to determine policy, and to have the authority to promulgate and enforce its findings on the military and industrial users who are charged with handling classified information in their computer centers."

(b) (1)
OGA

In an effort to establish such an authority as he described, Ware turned to NSA. As a result of correspondence between he and Carter, [redacted] also suggesting that NSA assume this role, a meeting of the NSASAB at Fort Meade was devoted to this question. It resulted in a formal statement, wherein;

"The NSASAB urges that the NSA assume its natural position of leadership and not take a parochially passive attitude to this emerging national problem."

The NSASAB pointed out that the problem was no longer confined to the "in-house" computing but extended beyond the Agency. The massive computer network shared by many government agencies and activities for the processing and dissemination of all classifications and types of information, some of which was common to all users, others highly restricted, had evolved. The Community On-Line Intelligence System (COINS) interfacing to the NSA RYE computer system was an example. Although it started out as a closed system where all the users were members of the intelligence community, it expanded to include other subscribers who were not authorized access to all classifications and categories of intelligence data, as was forseen by the NSASAB in prior advice to the DIRNSA.

The "role" paper called for a decision to be made soon as to the scope and involvement and responsibility of NSA. The need for such a decision had been given impetus by repeated inquiries to the Agency from a wide variety of government users for assistance in the installation of multi-access computing complexes which processed classified information. It was given urgency by planning for implementation of the World-Wide Military Command and Control System (WWMCCS), an on-line data exchange system handling all levels of classification and employing hundreds of computers. It was given emphasis by the proposal for a new USIB Committee on Information Handling, with the mission to foster research, establish procedures and standards and determine requirements for the development of community information handling systems.

BACKGROUND FOR ENLARGING THE SCOPE AND MISSION OF COMSEC

The NSA has been involved in the area of COMSEC evaluation of computer controlled communications systems since the late 1950's. In this application the computer generally exercised a pre-programmed set of instructions to determine the acceptance and disposition of traffic based on certain variables contained in the header. The control program could be altered only by the supervisor under strict parameters. A remote terminal could only enter units of traffic of classification levels for which it was authorized for onward delivery by the system as stipulated in the header.

Subscribers were not permitted to directly alter information, programs, or data stored within the computer. They received and requested only those communications for which they were a designated addressee. Also, subscribers were authorized access based on classification and category of the information.

The drafters of the paper felt that the concerns of computer security were similar or the same as that encountered in the communications security field. They presented their view of computer security needs and remedies to some of the problems by describing data processing activities they experienced.

Some of those security concerns, of a duality nature, were the protection of the transmission path by the use of cryptoequipment and protection against spoofing. Spoofing is defined as an attempt to gain access to a system by posing as an authorized user. Synonymous with impersonating, masquerading or mimicking. The user and remote terminal must be authenticated for the classification level involved. There must be preventive measures against unintended header designators due to transmission, software and hardware, or operator error and detection of such an event. The communications content must maintain its integrity while traversing throughout the system and while undergoing read and write transactions in memory. There is also security concern regarding emanations commonly referred to as TEMPEST i.e. the study and control of spurious electronic signals emitted by electrical equipment.

The COMSEC role at NSA included assistance in the provision of cryptographic equipments for the communications transmission paths and the analysis of traffic flow. Also, COMSEC was responsible for the evaluation and verification of software and hardware to insure compliance with established COMSEC standards and criteria.

NSA conducted Communications Security evaluations on computer applications that were engaged in command and control applications. This was an extended use of the communications systems whereby the computer was not only controlling the delivery of traffic but was also exercising the information content of the communications traffic. In this situation, the computer caused an effect based on a decision and verification of the information input. The effect may be direct activation and control of some mechanism or display of command influencing the data. Here, the computer operates under a pre-programmed set of instructions which could be accessed and altered only by the system supervisor under stringent controls. Generally the flow of information was one way; from the lower echelon remote terminal to the command center. The remote user was not permitted to receive or request recall of stored data.

In addition to the NSA efforts in the COMSEC evaluation of computer controlled communications, command and control, and cryptographic systems, the Agency had informally provided guidance

when it came to computer security in information retrieval and data processing systems. The guidance was given only upon request from various elements of the Department of Defense and other U.S. Government agencies. Experience had shown that most system planners recognized the need for protection of classified data in the multi user systems. However they had nowhere to turn in seeking any guidance for handling different classification levels of information within a single computer. The advent of time sharing systems further complicated the situation.

Data processing systems presented the greatest challenge to the task of providing and maintaining information security. This was so because the remote terminals used the central processor to execute their own software routines. Extreme caution was to be taken to prevent the remote stations in their programming and debugging activities from affecting, in any way, the operating system of the central processor. Some examples of how protection could be provided were through the use of memory locks, bounded memory for the suscribers' use, read and write only memory areas and physical security measures for the equipment.

Systems that were constrained by the use of information retrieval only, generally presented a lesser security concern. However, special attention was given to verification of authority to access particular information. This could be handled similar to the communications systems wherein a remote terminal received only that data to which it was authorized provided the user entered the proper password or key. The remote terminals were not permitted any programmable functions and could only request delivery of files based on the predetermined parameters they were provided.

DEFINING THE NSA ROLE

Three alternatives were presented. The first was named the decentralized approach. It would allow various NSA staffs to develop broad guidelines and contribute to the establishment of policy that would be promulgated to the military departments and federal agencies. However, each receipient of the policy was required to provide trained staff to implement the requirements. Protective measures could be established on the basis of assessing the risk associated with the operation of the equipment in a particular application and setting. Security in future equipment design could economically be achieved by NSA providing minimum essential criteria to government organizations. In turn, the government organizations would incorporate the security criteria in their instructions to the manufacturers and systems designers.

The second alternative was called the centralized approach; addressing the solution of specific security problems. It would entail the evaluation and direct guidance to the user when resolving security weaknesses in every area; e.g. personnel, hardware/software, communications and TEMPEST. A large workforce, experienced in COMSEC and computer hardware/software, would be

required. NSA would test, operate and evaluate entire systems with a resulting solution to retrofit or modify systems on a case-by-case basis.

The last alternative can be characterized as a limited effort. It would be primarily devoted to providing crypto equipments for communication paths connected to the terminals, switches and outstations.

CONCLUSION AND RECOMMENDATION

First, NSA specifically needed to make known its' position regarding the extent of involvement and support of computer security. The traditional role of providing COMSEC to communication switches, command and control and cryptographic devices needed to be restated in order to dispel any doubt or misinformation. The basic issue was to address the concerns of the information retrieval and data processing systems.

A recommendation was made. The authors recommended the adoption of the decentralized approach. The NSA role should be designed to shrink its' actual involvement as other government departments and agencies acquire knowledge and capability in computer security. The Agency should begin with a broad approach to fill the present vacuum and then diminish the role over a specified period of time. NSA should encourage the rest of government to acquire and train personnel and apply their knowledge to the computer security problems within their agency. This recommendation was believed to be in consonance with the recommendations of the NSASAB.

STAFFING THE ISSUE WITHIN NSA

The policy staff (D4) recommended the compilation of a list of computer systems, in priority order, from which NSA could provide assistance during the early stages of involvment. Limited NSA capability would be applied in accordance with the list. This implied that only the more important systems would receive NSA help and the lesser priority systems would be left to the capabilities of the parent military service or federal agency. They believed this approach would moderate the work load and prevent a massive build up of Agency capability against an impossible workload.

D4 felt that the promulgation of Computer Security policy and regulations within the DOD could be handled in DOD publications. As regards the rest of the federal government, a National Security Council policy document would suffice to address that need. The needs of industry were met through the promulgation of the Industrial Security Manual.

The data processing organization, known as C group, felt

that the comments of the R&D organization were particualrly meaningful (commentary to follow below). C group feared the imposition of extreme unrealistic and unreasonable security parameters upon the NSA computer plant. The organization felt that it was possible to operate computers in the multi-level and multi-programming enviornment in a secure fashion. This could only be accomplished with realistic adjustments to the environment, work flow and demands of the particular problem.

C group believed there was no general solution to the computer security problem. For example, physical security personnel were presented with general guidelines which they were expected to apply in a detailed fashion to a particular installation or problem at hand. The same concept applied to the computer environment with an additional problem that the number of technicians who truly understood how the monitors and executives of large scale systems functioned, was extremely limited. Further, the technicians were occupied with getting the system running and keeping it running. They were not inclined to devote a great deal of time to the security considerations. It was important that security considerations be answered specifically by people trained in the computer arts and not by a professional security operator.

C group believed that it was mandatory that NSA find an approach to the security problem. Many actions were being taken outside the Agency which could significantly direct or alter the final government wide solution of computer security problems. For example, the ARPA activities and the proposal to have Ware head a task force for the solution to this problem. NSA should have a very substantial and well established internal position for interfacing to these outside organizations. The NSA problem was fairly massive, in some ways unigue, and could not be handled if overburdened by a compromise to a general solution. It was imperative that the NSA position be made clear inhouse and that it be properly represented to outside groups.

The C group opinion of the proposed NSA role was that it did not address the real issue of computer security. It only addressed large scale batch machines which were shifted from one security level to another. The real computer security problem existed in the multi-access machine with a muti-programming or time sharing executive. It was this sharing of control by multiple programs, each of which had a different clearance level or each of which had a different end goal that presented the problem. As to the COMSEC recommendation for development, testing, authentication and continued surveillance for accuracy of the monitors, C group declared that it was a very severe administrative problem. The S approach handled only the questions of communications and authentication. It was felt that it gave too little attention to the internal problems of the management of the individual mechanisms to guarantee internal security.

The Research and Development organization had no specific responsibilities or technical tasks that included computer security

as a primary objective. However, as evaluators and developers of computer and information systems, they were keenly interested in the subject. They provided the following comments as to the NSA role.

"...The most important thing that NSA should do at this time on this subject is to take a position on what it is willing to do, if asked, and to assign Agency-wide responsibility internally. Because of NSA's responsibilities and capabilities in communication security, its heavy involvement in the computer systems field, and its long practice at handling internal information security problems, other government agencies and their contractors naturally turn to NSA as a source of guidance. NSA can only look foolish if it continues to avoid taking a clear policy position which defines in what manner it will participate in the discussion and solution of these problems. The present situation places individuals who get involved in such discussions in an extremely awkward position. The failure of NSA to participate in some meaningful fashion could result in the development of standards that would apply also to NSA, but which were not palatable for some reason..."[1]

R&D felt the decentralized approcah was the best alternative discussed. However, it offered what it believed to be a stronger approach. R&D proposed that NSA should be willing to develop and be responsible for standards for computer system security; to include government wide scope. NSA should not be a policing agent! Although, at first, it should be a training agent. Then, it should test and demonstrate the standards in operating systems that it owns. NSA should be a center for technical consultation in system security and problems. It should demonstrate the application of standards. The centralized approach and the limited effort approach were undesirable.

The final remarks, regarding the "role" paper, came from the pen of David G. Boak, former Chief S13, an organization concerned with the physical security aspects of the COMSEC arena. Mr. Boak words appear in quotes below as excerpted from his memorandum of 15 November 1967 to S06.

"... I am reluctant to endorse the notion of Dr. Ware having any lead role with respect to the problem. From what little I know of his views, I would be afraid that he would drive towards an overcommitment of the Defense Department in general and NSA in particular in solving many aspects of computer security design problems that more properly should rest with industry or with non-DOD computer users - "privacy" for business and personnel information processed by computers, for example. I would also fear

---

[1]Memorandum from R55,Ronald L. Wigington to S06, dated 29 August 1967, Subject: The Role of NSA in Computer Security

pressure to declassify or proliferate (with the same effect as declassification) information on the more subtle vulnerabilities of computers to exploitation, and on sensitive countermeasures used...

... I see a fairly close analogy between the ADP security problem and that of TEMPEST. Because we had a deep concern and our own systems, equipments, and installations were affected, and we could be fairly characterized as least incompetent in the field, this Agency by 1960 had assumed a lead role in TEMPEST matters. We had our hands in policies, standards, testing, training, some policing, countermeasures, and R&D not only for CRYPTO and SIGINT-supporting hardware, but for the whole gamut of information-processing devices suseptible to the phenomenon. Experience showed us rather quickly that we had bitten off too much; and much of our effort for the last several years has been to effect disengagement and delegation..."

In closing, Boak believed that there was an underestimate of the resources necessary to carry out the proposed responsibilities. He felt that the sanitization and deguassing problems were more formidable than the paper implied. Finally, he judged that NSA could not obtain any additional resources and in fact he opined that NSA should not even try.

The general consensus amongst the respondents was to not seek additional responsibility beyond the established charter and mission of the Agency. This view prevailed in practice and policy throughout the Agency for another twelve months until 13 December 1968 when another study on the role of NSA in Computer Security appeared. This effort, again initiated by the COMSEC organization, would culminate in a new policy that would direct the Agency on a path of active engagement in security of data processing.

In order to understand this change of heart, we must first examine the events that took place in that year of 1968. NSA had, for a very long time, the responsibility for communications security in the U.S. Government. The evolution and resultant capability in COMSEC had been gained through experience. This experience had brought exposure to computer systems as information systems evolved into the utilization of computers for communications. Therefore, NSA was presumed to be a natural source of computer security guidance as perceived by other government organizations. Due to the prevailing philosophy at NSA, the Agency had tried to limit its involvement in computer security to the solution of problems related to the use of cryptographic devices. This approach to the subject appeared appropriate due to the lack of trained people and the absence of specifically defined responsibilities outside the NSA. Although the COMSEC involvement was limited, other NSA activities were gaining considreable expertise, particularly in the computer organization and this was not going unnoticed outside the Agency. This limited involvement and capability on the one hand and the recognized expertise in computers on the other hand was difficult for people outside of NSA to reconcile.

The COMSEC effort continued to be expended on varied and sometimes naive requests from outside the Agency. The guidance and assistance was concerned with messages, message format, procedures, software and other problems related to ADP system security. This activity placed the Agency and individuals who were involved in such actions in an awkward position because the COMSEC personnel lacked the knowledge and preparedness. They did not properly respond but reacted to the outside requests in an attempt to be cooperative and yet adaptive to varied requirements as they happened.

Here are some examples of the time shared systems that requested technical assistance of NSA.

NSA personnel participated in the Joint Technical Specifications Group established by direction of the Deputy Secretary of Defense. Its' task was to prepare specifications and supporting material for industry wide competitive selection of ADP systems to update the World Wide Military Command and Control Systems (WWMCCS). NSA was tasked to provide the policies, procedures and specific criteria which were to be used in safeguarding multi-level security data employed in the WWMCCS and the Intelligence Data Handling System. These systems were on-line data exchanges that handled all levels of classification and employed hundreds of computers.

The Director, DIA, in April 1967, proposed that a new USIB committee be established on information handling. At its 4 April 1968 meeting, the United States Intelligence Board (USIB) approved the establishment of this committee and a set of objectives for intelligence information handling were enumerated. The objectives included development of rules and procedures for handling information; development of a coordinated R&D program and specifically, develop new security standards to assure the protection of intelligence information incorporated in automatic data processing systems, particularly multi-programming and on-line systems. NSA by virtue of its' USIB membership was obligated to assign personnel to this committee named the Information Handling Committee (IHC).

At the request of DDR&E, an Ad Hoc Group was formed by the Advanced Research Projects Agency in September 1967 to establish a DOD task force to define and study the problem of security in a resource sharing environment and to submit solutions and costs. A Steering Group and two working panels were established. NSA was prevailed upon to Chair a Policy Panel (in addition to providing members on the Panel) and to provide members for a Technical Panel. The Policy Panel was charged to state what logical or doctrinal limitation should be placed on use of time shared facilities for security reasons. The Technical Panel was asked to describe the hardware and software capabilities available or required for implementing a time sharing system under the policies given by the first panel. In May 1968 the task force was formally titled the Defense Science Board Task Force for Securing

Time Shared Systems. The DDR&E goal although limited to developing policy for use in the Department of Defense, expected any success achieved to attract other parts of the government.

As for the other side of NSA (Intelligence), the activity in computer science and security was attracting the interest of outsiders. NSA had achieved considerable competence as a result of in-house programs like RYE, TIPS and COINS. RYE was the highly sophisticated NSA UNIVAC 490 and 494 computers that provided analytical personnel with remote access to computers from their work area by means of data input and output terminals in a time sharing mode. The Technical Information Processing System (TIPS) was a major system operating on RYE that provided rapid information retrieval for SIGINT management, long and short term analysis and research. In compliance with White House directives, a secure computer system was planned for in the USIB Community to improve interchange of information. The project was known as the Community On-Line Intelligence System (COINS).

Agency personnel were participating in the security testing of the ADEPT-50 computer time sharing system. This system was composed of an IBM 360/50 computer and many software programs. The ADEPT-50 system was sponsored by the Advanced Research Project Agency for the National Military Command System with the mission to help support the military command and control data processing activity at the Pentagon. Users of the ADEPT-50 system had different compartmented clearances. NSA was asked to provide support and make recommendations regarding the securability of the ADEPT-50.

The emerging proliferation of shared computer systems prompted a broad categorization of such systems. There were basically two; the first was a shared system that required no communication outside a controlled area; and the second was a shared system linked over secure or protected lines to distant computers and out stations. This traditional configuration of shared systems was now evolving into a new situation of integration with telecommunications systems from which secured and unsecured lines radiated.

What was evident in all of these systems was the requirement for protection of information in an ADP system that was readily accessible to all of its users. However, a general rule that had emerged was the practice of users, with various clearance status, using computer to computer operations and remote access stations located in protected and unprotected areas. This practice fostered the notion that concern for security was adequate if one secured their portion of the system or network. The users failed to recognize and understand that their portion of the system was connected to a much larger system or network that required equal if not greater security protection. Failure to secure the entire network caused an individual stations' files and data to be subject to manipulation. In all of this, the authoritative NSA role, as defined in Director of Central Intelligence Directive 6/3 (DCID

6/3), for exercising security controls, was only when the system was processing SIGINT (Siginals Intelligence) or utilizing crypto equipment. Thus, the question was asked again, what is the policy on the NSA COMSEC role in computer security? It would be very desirable for COMSEC to state its' involvement in computer security and thus control future activity to manageable proportions.

The National Security Council Directive (NSCD), dated 26 August 1968, stated that "COMSEC is concerned with all measures designed for the security of federal telecommunications". The Director, NSA, was charged in the NSCD to "evaluate and advise the Board (United States Communication Security Board) and department and agencies concerned on vulnerability of telecommunications to hostile exploitation, recommend basic doctrine, methods, and procedures to minimize COMSEC vulnerabilities." "However, if we attempt to take over the whole of the problem area, we are almost certainly asking for trouble and a task which we are not ready to perform."[1]

The concern for industry was recognized in its desire to produce computers that would fit the requirements of the government. Additionally, industry liked spin-offs from the government that would help it in arriving at privacy techniques that would benefit their commercial customers. It was noted that neither of these industrial objectives fell within the purview of the National Security Council (NSC) COMSEC Directive of 26 August 1968.

Finally, the NSC Directive stated that nothing shall relieve the heads of the individual departments and agencies of their responsibilities for executing all measures required to assure the security of Federal Telecommunications. The protection of a shared computer system against use by unauthorized persons fell within the responsibilities of the individual departments and agencies. Protection responsibility and segregation of information within the computer complex was identical to the usual and accepted responsibility of a USER to protect information stored in a container during non-working hours. Equal responsibility applied when the information was not under the direct and continous control of properly cleared and authorized personnel. The aforementioned statements depicted the interpretation of the NSC Directive by the COMSEC organization when it came to the safeguarding of classified information resident in computer systems. The continuing philosophy was for NSA to promote individual departments and agencies to provide for their own data security protection.

On 23 December 1968 draft policy designed to provide guidance to the NSA COMSEC role in the area of computer system

---

[1] A STUDY OF THE NSA ROLE IN COMPUTER SECURITY, dated 13 December 1968.

security was circulated for comment. The draft policy was the result of the Study of the NSA Role in Computer Security dated 13 December 1968. The declaration of the draft policy asserted that the COMSEC role would be consistent with the objectives, policies and procedures in the National Security Council Communications Security Directive (NSCD), dated 25 August 1968 and Annex C to DCID 6/3, dated 21 July 1967.Therefore, the COMSEC organization had responsibility in two of the computer security applications. First, those applications in which the computer was or would be performing a cryptographic function and secondly, where the application of the computer was part of a telecommunications system.

NSA exercised the full range of responsibilities and authority when the computer application was performing cryptographic functions. However, for those applications in telecommunications systems in which the computer did not perform a cryptographic function, NSA would collaborate with the cognizant department or agency. In the evaluation of such systems, the detailed collection and analysis of data was to be performed by the cognizant department or agency and the NSA role was limited to providing guidance and criteria for the evaluation. It should be futher noted that the foregoing responsibilities were applicable only in fulfilling the requirements of the Federal Government.

So, from January 1969 to October 1969, the aforementioned study and several iterations of draft poicy on the subject of the role of NSA in computer security were coordinated amongst the operations organization, the administrative organization, the research and development organization and the communications security organization of the Agency. Finally, on 14 October 1969 Tordella issued a policy on the NSA Roles and Responsibilities in the Field of Computer Security. Tordella stated that this policy was promulgated for the use of Agency elements involved in the use of computers and associated ancillary equipment that processed classified information.

In the coordinating effort of drafting this policy, C group, the computing organization of Operations Directorate, provided some interesting insight as to the state of computer security within NSA at that time.

"...Security in general is a controversial subject, but when security becomes involved with computers it brings forth problems never before contemplated..."[1]

For over a decade C Group had been addressing the many problems of security in NSA computing systems. It was clear that 3rd generation, multi-user, multi-processor, time sharing, remote access systems posed complicated hardware and software problems.

---

[1]Memorandum from C Group to Assistant Director for Production, Subject: Handling of Compartmented and Sensitive Information in Third Generation Computer Systems, dated 5 June 1969.

However, C felt optimistic that the threat could be reduced to an acceptable level. But, it felt that it was not possible to establish a meaningful overall security policy at that time. In reality what was happening was the establishment of "policy-by-precedent", learning as we go.

The state-of-the-art in computer technology, especially a trend towards manufaturer integrated hardware-software systems, made C more and more subservient to the delivered system. This remained true and became the dominant influence in all future NSA systems. Each unique computer system was measured independently against security criteria that was unique to that system. Each case became a trade off between what constituted an acceptable level of security and the computer time, manpower and monies expended for its implementation and continued usage. In very demanding situtations, (i.e., the NSA RYE system), elaborate security procedures with their incumbent costs was warranted while in others less complex and costly measures would suffice.

C group believed that the RYE system was the only resource sharing system within NSA which had implemented a full multilevel security system. The system was implemented within the security requirements of existing regulations and was considered secure enough to process classified materials. However, the Chief of C, E. [redacted], was quick to point out, "...nevertheless I would not hook up a [redacted] to RYE..."[1]

"In light of the industry wide efforts to cope with computer security, C recommends further study before attempting to formulate all inclusive policy. The NSA should continue to gather statistics from RYE, discuss the successes and failures with others having comparable systems..." [11] Appendix C contains a copy of the 1969 policy on Computer Security at NSA.

(b)(1)
(b)(3) - 50 USC 403g Section 6 of the CIA Act of 1949
(b)(3)-50 USC 3024 National Security Act of 1947 Section 102A(i)(1)
OGA

(b)(3) - 50 USC 403g Section 6 of the CIA Act of 1949
(b)(3)-50 USC 3024 National Security Act of 1947 Section 102A(i)(1)
OGA

[1]Ibid.

[11]Ibid.

OTHER EVENTS

Some interesting parallel events took place at about the same time the NSA computer security policy was in formulation. As with any major change to a culture, the computer was no exception, its' introduction into the work place fostered an evolution of change. The universal introduction of the computer into the intelligence community sparked additional concern for the security of the data therein. The United States Intelligence Community was guided by a United States Intelligence Board that had various committees devoted to the formulation of policy in areas of concern to the intelligence Agencies. Some areas of concern were Information Handling, Sigint, Humint, Communications and Security. It was here in the Security Committee that a working group concerned with Computer Security evolved into a permanent subcommittee of the Security Committee. The charter of the Computer Security Subcommittee was comprised of two elements:

First, to recommend to the Security Committee those policies, methods and procedures considered necessary to provide adequate security protection for all ADP operations in the USIB member organizations; and

Second, to serve the Security Committee, other appropriate USIB components and individual USIB members in isolating and recommending solutions to security problems in the ADP environment as they arose.

The Subcommittee became very active in its zeal to achieve its objectives. Its activities were perceived by NSA as increasing demands on the Agency for further involvement and assistance. The Subcommittee identified security problems in many areas; some were traditional security, some were purely technical security and others were a blending of the two. The NSA member was an employee of the Office of Security. In many instances the NSA member solicited assistance from other elements of the NSA possessing the required knowledge. For example the NSA member was named as the chairman of a task group to research and write specifications for the sanitization of computer storage media. After discussion with knowledgeable Agency personnel, it was agreed that this task was not within the realm of achievement by this task group; resulting in the withdrawl of the charge. Later, NSA promulgated an internal paper on the degaussing of computer magnetic storage media and the Subcommittee adopted the essence of the paper and published it as guidance for the intelligence community.

In the Spring of 1970, the USIB Computer Security Subcommittee, wrote a draft proposal for a new Director of Cenrtral Intelligence Directive entilted "Minimum Security Requirements for Muti-Level Operation of Resource-Sharing Computer Systems in a Benign Environment". The purpose of this directive was to prescribe basic USIB policy concerning the security aspects of remotely accessed, resource sharing computer systems for the concurrent

processing and/ or storage of classified information. The document specified the conditions under which such systems operated in a multi-level mode and prescribed minimum security requirements for the operation of such systems. The directive assigned the responsibility for the security analysis, test and evaluation as well as the accreditation of such systems to the individual USIB members. This document was known as DCID 1/16.

On another front, in the early spring of 1970, Dr. Willis H. Ware, in his role as a member of the Defense Science Board, issued a final draft of the "Task Force on Computer Security" as mandated by the Office of the Director of Defense Research and Engineering. This effort was initiated when the question of security control in resource-sharing systems was brought into focus for the Department of Defense by a series of events in the spring and summer of 1965. Systems were being procured in increasing numbers for government installation and the problems of security became a pressing concern for the defense contractors and military operations. Consequently, the Research Security Administrators had forwarded a position paper [redacted] to the Director for Security Policy in the Office of Assistant Secretary of Defense (Administration) soliciting action. Since the matter involved technical issues, the paper was referred to the Office of the Director of Defense Research and Engineering for consideration.

(b) (1)
OGA

In June of 1967, the Deputy Director (Administration, Evaluation and Management) requested the Director of the Advanced Research Projects Agency (ARPA) to form a task force to study and recommend hardware and software safeguards which would satisfactorily protect classified information in multi access, resource sharing computer systems. The responsibility for this task, within ARPA, was forwarded to Mr. Robert W. Taylor, Director of the Office of Information Processing Techniques.

During the summer and fall of 1967, a series of discussions were held amongst individuals from the university and industrial communities; culminating by October 1967 in the formation of a Task Force comprised of a steering group and two panels. An organizational meeting was held the following month; thereafter the panels and Steering Group met on a regular basis to formulate the recommendations which constitute the body of the report.

The report contained many recommendations of use to designers, implementers, certifiers and operators of secure systems. The purpose of the Task Force was to determine the problems of creating secure time shared systems. As a part of this Task Force a technical panel was established. This panel met frequently during late 1967 and into 1968. The work culminated in a workshop held from 28 to 30 March 1968 at the Communications Research Division of the Institute of Defense Analysis at Princeton, New Jersey. The technical panel advised on the research areas that required pursuit in order to guarantee the security of

resource sharing systems. Four primary research areas were recommended.

1. Security structure language. The design of the security structure language should be completed and its implement algorithm defined.

2. Consistency checks. A rapid early analysis should be made of the possibility of incorporating hardware consistency checks in equipment supplied by major manufacturers.

3. Systems certification. A research program should be delineated for the problem of determining the feasibility of more automated, hence exhaustive, certification of the integrated hardware and software system with due regard to its operational environment.

4. Cryptologic research. A program for the necessary cryptologic research in order to facilitate the early availability of secure time sharing systems.

Also, during the month of May 1969, a final report appeared on the scene entitled "Computer System Security Techniques" prepared by the James P. Anderson and Company of Fort Washington, Pennsylvania, a consulting firm in computer security. This NSA awarded contract called specifically for the following:

a. A study and description of criteria for assuring a specified level of security in a multiple user computer system.

b. A survey of security safeguards in existing or proposed time sharing systems.

c. An evaluation of the survey findings in sufficient detail to be used by NSA in developing criteria and system design principles to provide adequate security safeguards on future NSA time sharing systems.

The report dealt with the issue of computer system security techniques as they particularly applied to multiple user systems. Several systems were surveyed; the IBM 360/67, the GE 645, the GE 635 and the UNIVAC 494.

Two very difficult problems emerged from the study and were essentially unresolved. First, all of the systems surveyed, to include RYE and the Defense Intelligence Agency ANSRS sytem were vulnerable to penetration and exploitation by operations personnel. There were no technical measures that could be taken to protect systems from unscrupulous operations and maintenance (hardware and software) personnel. Second, there was no mechanistic way of verifying the correct design of the operating system.

The above described activities, occuring on many fronts, served as added impetus for NSA to declare a position and establish

a policy on its role in the computer security arena. As was previously stated this publicly declared policy of the NSA involvement in computer security was to be confined to the problems associated within the Agency and only would NSA involve itself in the external world when COMSEC requirements were clearly indicated. This policy was to remain in effect for approximately two years; thereafter, the policy was revised. However, before we continue with the NSA story of its involvement in computer security lets turn to two major studies that were previously mentioned; that is the James P. Anderson and Company study entitled COMPUTER SYSTEM SECURITY TECHNIQUES and the Report of the Defense Science Board Task Force on Computer Security entitled SECURITY CONTROLS FOR COMPUTER SYSTEMS. Because the studies involve the NSA, the former directly and the latter indirectly, they further illustrate the continuing pressure toward the NSA to become involved in a more meaningful way. The next two chapters present the essence of those efforts.

Chapter 3

COMPUTER SYSTEM SECURITY TECHNIQUES OF "THE PERIOD"

This effort was accomplished through the award of a contract by NSA to the James P. Anderson and Company. The contract was for the period from 16 April 1968 to 16 April 1969 with the final report presented to NSA on 16 May 1969. The contract requirement called for the examination of computer system security techniques as they particularly applied to multiple user systems. The specifics called for:

* A study and description of criteria for assuring a specified level of security in a multiple user computer system.

* A survey of security safeguards in existing or proposed time sharing systems.

* An evaluation of the survey findings in sufficient detail to be used by NSA in developing criteria and system design principles to provide adequate security safeguards on future NSA time sharing systems.

The survey included the following systems:

IBM 360/67 (TSS)

GE 645 (MULTICS)

GE 635 (ARK)

UNIVAC 494 (RYE)

SDS 940

The lack of available information on the SDS 940 caused the machine to be dropped from the survey.

The survey revealed a minimum of security requirements that must be present if the system was to provide adequate secure handling of classified information. The system must have:

A physically secure environment for the computer, remote terminals and other physical elements of the system.

Control of access to the system.

An adequate method of internally isolating individual simultaneous users of the system.

A protection mechanism for the program and the data file subsystem; and

Protection against inadverent disclosure.

Each time-sharing system must be evaluated on its own merits regarding the above requirements. Failure of a system to adequately meet any of these criteria was sufficient to declare it insecure.

The study defined the scope of the security problem in time-shared systems as a function of the degree of direct control of a system, the level of material being handled and the clearances held by the user population. Any variation in these elements would change the nature of the security problem and possibly the steps necessary to secure the information processed.

Recognition of the security threat among systems where direct user control existed was a function of the direct user control possible in a system. Clearly, if a user at a terminal could not exercise direct control over the program that was executing, then the user was less likely to be able to cause improper operation of the program versus a user who had a high degree of direct control.

The study recognized a number of points along a spectrum of direct control. That spectrum ranged from transaction systems to remote accessed resource time-sharing systems.

An example of a transaction system was one in which only specific 'canned' programs could be used from a terminal, for example an airlines reservations system. Here the user 'control' of the programs is limited to supplying the parameters.

Then there were the systems that provided interpretive computing for the terminal user. An example was a system that provided for the utilization of a language such as BASIC. The principle distinction was that although the user could specify in some detail both the functions to be performed and the sequencing desired, the user was barred from direct control of the hardware. The user was not permitted to write instructions that were directly executed by the machine. When the user executed programs through the use of an interpretive language it was a fact that the operations and the sequencing between steps was interpreted by another program standing between the user and the hardware of the central processor. Also, interpretive systems isolated users from the knowledge of memory allocation functions.

The study focused on systems that used only approved compilers to produce running code. It singled out the outstanding example of this kind of system as the Burroughs B5500 which presented the machine to the users only in terms of the Algol, Fortran and Cobol compilers. No assembler existed for the system.

Anderson examined systems that permitted the user at a remote terminal to write in the machine language of the system and execute direct debugging control at the machine language level. The 'machine' language was most frequently the assembly language. Examples included machines manufactured by IBM particularly the 360/67 and the General Electric 625 and 635 with Gecos III as the operating system.

As a matter of practicality, most timeshared systems offered a range of use encompassing nearly all of the above cited cases. The security problem increased as the installation opted to permit more direct user control.

The survey examined the hardware for secure resource sharing systems and discovered that in large measure those features that facilitated the design and proper operation of real time multi-programming operating systems were the driving design goals. The designer was preocuppied with delivering a product that was advertised to perform the functions so named in as efficient and flawless manner possible. Security was a secondary consideration, if at all.

The balance of the report discussed and illustrated specific technical steps that could be taken to provide resource sharing systems security.

The report highlighted the kinds of security controls enforce to protect the information that was processed in the system. As a matter of illustration, the NSA RYE system was highlighted to demonstrate the kinds of security measures employed to protect the system. However, the reader is advised that there were variations in the kinds of security features in force in the other systems. To acquaint yourself with those security structures, the reader is referred to the Anderson study. Incidently, the first manager of the RYE system, Bernie Peters, was a 'teetotaler' with a sense of wit for the au contraire and named the UNIVAC 490/494 system RYE as in whiskey.

The goal of the RYE security procedures was the prevention of unauthorized disclosure of information which was stored or processed in the system. Improper transfer of information was the most significant danger to the secure processing and storage of classified data.

The RYE system had been assigned the mission of serving segments of the cryptologic and intelligence communities. This was accomplished by operating and maintaining a centralized, coordinated collection of computer equipment for on-line computation and information storage, retrieval and processing. Also, the user was provided with remote access. Security for the system was tailored to that mission, protecting the system, but not restricting it unreasonably.

The security problem in the RYE system was unique and more

difficult to accomplish because the system stored and processed, simultaneously, several compartments and levels of classified information. The problem was not one of merely protecting the whole body of sensitive information but, just as importantly, one of appropriately segregating the information within the system.

The security structure for the RYE system was based upon a composite of physical security, machine security, and communications security procedures.

The RYE system controlled access by physically controlling access to a terminal. Also, the RYE system used a terminal clearance technique to control access to the system. Each outstation (terminal) had a clearance level and only jobs up to that clearance level were initiated from that terminal. As a consequence, RYE security was unique because it provided the same security attributes to the terminals that were attributed to users in other time-sharing systems. It was always assumed that a user who logged on a RYE terminal was permitted access to the system and in particular, the program set that could be activated from that terminal. This approach to system access control greatly simplified the maintenance of access controls in the RYE executive, since it must only establish clearances for the terminals in the system and not for the myriad of users who could use the system. It also alleviated the necessity to maintain an elaborate password mechanism.

By adopting the approach of controlling access to the system through controlling physical access to terminals and giving terminals security attributes, the flexibility of the system was reduced. If a particular file owner wished to grant access to his/her files to a user in a remote location, he/she did so by modifying the security attributes of the terminal in that remote location. This access permission exposed his/her files to any user who could gain access to that terminal.

The idea of assigning security attributes to terminals was useful in an environment where a like-cleared group of users were sharing a set of files and programs and had no requirement to deal with other groups, particularly those located remotely.

The RYE File System provided for various access controls through a system of security flags. The security flags codified the security attributes of different objects in the RYE system. The objects were: terminals, files and programs. All access to program and data objects was controlled through matching security flags of a terminal against the security flag of the program or file. Since programs were the mechanism for accessing files and other programs, an access was completed in terms of the security flag of the terminal initiating the job in which an access attempt took place.

In the case of files, an additional level of access control was employed. Not only must the security flag of the program attempting access match the security flag of the file, but

the terminal originating the program must have been registered on the file's access list. This limited access in those cases where the file classification was common, e.g. SECRET, and would presumably be potentially accessible from a large number of terminals. The RYE system also accomodated a general use data retrieval system.

The general use data retrieval system was called the Technical Information Processing System (TIPS) and it operated as a RYE job. The TIPS security features were based on those in general use in RYE. TIPS requests were interpreted by a TIPS supervisor as a set of calls on TIPS and RYE worker programs. The files that were retrieved or updated ran the gamut of classification; therefore, the requesting station security flag was the security flag for the request and was 'attached' to the various TIPS programs. This differred from ordinary RYE operations where the worker programs had their own security flags that were matched against the flag associated with the requesting station before the job was initiated.

Access to TIPS files was controlled by matching the security flag of the originating station against the security flag for the file. Control of the type of processing allowed was achieved by associating with each file two links. One link for those terminals permitted to retrieve from the file and the other link to those terminals permitted to update the file. A further check was also imposed on the authority of a terminal to perform the type of operation indicated by the request.

In summary, the net effects of the TIPS security mechanisms were:

A TIPS message would be processed by TIPS only if the remote station originating the message was on the appropriate access list of every TIPS file cited in the message.

A remote station could receive TIPS output only if the receiving station was on the extract access list of every file cited in the message ordering the output.

A remote station could receive TIPS output only if its security flag was higher than or equal to the security flag of the remote station originating the TIPS message which prescribed the output station.

In summary, RYE was designed to control information transfers to, from and within the system in such a way that information was passed only upon the authorization of its owner.

Ownership and identification of files, programs and remote stations were represented by the security flags assigned to those items. The security flag relation file expressed the access authorizations associated with each flag. An owner could grant access authorization on the basis of clearance level or need-to-

know or both.

For the purpose of controlled information transfer, RYE uniquely identified all remote stations, programs and permanent files. Access to the system from remote stations was based upon the station identity and not on the identity of the individual user operating the station. An individual's right to operate a remote station was decided by the authority responsible for the physical security of that station.

Information contained in a permanent file was not "classified" as such. The RYE system controlled access to a file in strict accordance with the access authorizations granted by the owner of that file. The access authorizations would certainly reflect the classification level of the information in the file, but the flag expressed that level only implicitly.

The executive program for the RYE system worked in conjunction with certain hardware features to force worker programs to pass all data tansfers, except those occurring solely within the core bounds of the worker program, through the executive programs. Physically separate data links ensured accurate identification of the remote stations. Redundant flags, duplicate checks of identities and flags, comprehensive logging and alert operators ensured a very low probability of undectected machine errors.

How well did the RYE system perform its security tasks? In December 1968, it was reported that RYE had been operational with UNIVAC 494 equipment since March 1967 and since that date had successfully processed over 500,000 RYE jobs and almost an equal number of TIPS jobs without security incident. It was stated that this operational experience sufficiently demonstrated that the RYE Executive program on the UNIVAC 494 equipment was capable of providing very secure operations. There were some cases of misdirection of output from TIPS jobs but this was attributed to the UNIVAC 490 equipment and the lack of memory protection features.

Although the eighteen month record of the operational RYE demonstrated an excellent security record, the managers were well aware that the system was not severly tested against sophisticated deliberate penetration attempts. RYE management felt that the only direct proof of security within the system design was from deliberate attempts by an adversary to penetrate the security structure. An adversarial test of the system was never conducted.

User activity at a remote station was restricted to activation of a worker program within the system. The worker program was completely controlled by the executive program which transferred information according to security flag relationships. Security flags and their relationships could not be altered from a remote station. The executive program could not be altered from a remote station. Therefore, remote station manipulation of the system was not possible.

The weakest point of the RYE system, as with any system, was the practical impossiblity of protection against the maintainers of the system. Although, the complexity of the system and the separation of programing, operating and maintenance functions made it very difficult to arrange an undetected penetration, there was very little one could have done to prevent it.

For example, the tapping of a particularly sensitive data link by a maintenace man or the reading of any printed page by an operator and also, the altering of the executive program by a system programmer so that a disguised copy of some particularly sensitive output was printed at his command. The worse case senario was the collaboration between two or more knowledgeable RYE employees; it could have lead to long term undetected compromises."

"A complete treatise of the security structure of the RYE system can be found in the "Security Procedures for the Rye System" by [redacted] dated 23 December 1968.

(b)(3)-P.L. 86-36

Chapter 4

THE WARE REPORT

The Department of Defense effort, although it received impetus from the concern that was generated by an ever increasing number of time sharing systems, addressed all computer systems that processed classified information.

The wide and divergent use of computers in the military and defense installations had long necessitated the application of security rules and regulations. The traditional approach for securing computer systems had been one of isolation; simply placing the entire system in a physical environment where penetrability was almost impossible. However, new security wrinkles had entered the picture with the geographical wide spread use of user terminals. Obviously, these problems were not solvable through elementary physical isolation.

It is important to note that the security problem was not unique to any one type of computer system or configuration; it applied across the spectrum of computational technology. Although the task force group, directed by Ware, emphasized the concern of time sharing and multiprogramming, the problem was not really about system configuration but about security.

Additionally, resource sharing systems, where the problems of security were most acute, must be designed to protect each user from interference by another user or by the system itself. It must also provide some sort of "privacy" protection to users who wish to preserve the integrity of their data and their problems. Thus, the fundamental problem for designers and manufacturers of resource sharing systems was the protection of information.

It was the intent of the task force to compile techniques and procedures that would be flexible and adaptive to the needs of any installation. Further, it was there intent that the general guidelines they had formulated not only be of use to DOD components but also useful to other government installations and contractors.

They observed that there were several ways in which a computer system could be configured to serve the user. The security controls were dependent upon the way the system was organized and the sensitivity of the data to be processed. The group examined two ways of observing the physical and operational configurations.

The first was the way the equipment was arranged and disposed. This organization is best depicted in Figure 1. The batch processing was the historical and prevalent mode of operation. The most important characteristic of single queue, batched, run to completion systems was that the system required no "management

awareness" from job to job. Sensitive information could be erased or removed from the computer quickly and relatively at no cost. Also, mass memory media containing sensitive data could be physically separated from the system and secured for protection. This characteristic way of configuring systems explained why the security problem was not urgent in the past.

The situation was very different in mutiprogramming, where the jobs were organized and processed by the system according to algorithms designed to maximize the efficiency of the total system.

The other way of viewing the types of systems is shown in Figure 2; it was based on the levels of computing capability available to the user.

The Type I, file query system, enabled the user to execute only limited application programs embedded in the system and not available for change. The user selected for execution one or more available application programs contained within the system.

The Type II, interpretive systems, provided the user with programming capability, but only in terms of input language symbols. These symbols did not allow the construct of internal machine language and thus prohibited the user from gaining control of the machine directly.

The Type III, compiler systems, provided the user with a programming capability that was limited in terms of languages which executed through a compiler embedded in the system. The instructions to the compiler were translated by it into an assembly language or basic machine language program. Program execution was controlled by the user; however, the user was limited by the compiler language that was available.

The Type IV, full programming systems, gave the user extensive and unrestrained programming capability. The user could execute programs written in standard compiler languages, create new programming languages or write compilers and embed them within the system. This allowed the user intimate interaction with and control over the system's complete resources other than that prohibited by information protecting safeguards such as memory protection, base register controls and input/output hardware controls.

The task force defined three major categories of system vulnerabilities; (1) accidental disclosures, (2) deliberate penetrations and (3) physical attack.

In the case of accidental disclosure, a failure of components, equipment, software or subsytems could have resulted in the exposure of information. This type of vulnerability was frequently the failure of hardware or software.

A deliberate penetration required the action of a threatening party. The pentrator was generally motivated by the

reward of obtaining information. Another possible motive of a deliberate penetrator was to render the system unreliable or unusable to the legitimate operator. Deliberate penetrations were active or passive. Passive methods included wire tapping and monitoring of electromagnetic emanations. Active infiltration was an attempt to enter the system so as to obtain information from the files or to interfere with the system.

Active Infiltration was one method for the legitimate user to pentrate portions of the system for which there was no authorization. The design problem was to prevent access to the files by someone who was aware of the access control mechanisms and who had the knowledge and desire to manipulate them to their advantage.

Another active infiltration technique involved the exploitation of trap door entry points in the system. The trap door entry points by-passed the control facilities and permitted direct access to the files. Trap-door entry points often were created deliberately during the design and development stage in order to simplify the insertion of authorized program changes by legitimate system programmers. The system programmer normally intended on closing the trap-door prior to operational use. Sometimes the programmer failed to close the trap door and this set up a vulnerability within the system that could be exploited. Unauthorized entry points could be created by a system programmer who wished to provide a means for bypassing internal security controls and thus subvert the system. There was also the risk of implicit trap-doors which existed due to incomplete system design. As an example, it was possible to find an unusual combination of system control variables which created an entry path around some or all of the safeguards.

Active infiltration could also be performed through the use of a special terminal illegally tied into the communication system. This terminal could be used to intercept information flowing between a legitimate terminal and the processor or it could manipulate the system. As an example, a legitimate user's sign-off signal could be intercepted and cancelled; then, the illegal terminal could take over interaction with the central processor.

Active infiltration could also be performed by an agent operating within the secure organization. The agent could cause what appeared to be accidental acts that caused disruption to the system or the users and could have resulted in the acquisition of classified data. Other agent acts could result in the obtaining of removable storage media containing classified information. The agent may also commit acts of subversion within the system for later exploitation.

The opposite of active infiltration was passive subversion. Here, the subverter applied means to monitor information resident within the system or transmitted through the communication lines without any corollary attempt to interfere with

or manipulate the system. The most obvious method was the wire tap. If communications between remote terminals and the central processor are over unprotected circuits, the problem of applying a wire tap to the computer line was similar to that of bugging a telephone call. Further, it was possible to monitor the electromagnetic emanations that were radiated by the high speed electronic circuits that characterized so much of the equipment used in computational systems. Energy given off in this form was remotely recorded without having to gain physical access to the system or to any of its components or communications lines.

In summary, the system vulnerabilities were depicted in a pictorial; see Figure 3. The threat points were summarized into five groups: 1) physical surroundings, 2) hardware, 3) software, 4) communications links and 5) organizational (personnel and procedures). This particular visual was entitled "Computer Network Vulnerabilities" and was extensively used throughout computer security education presentations. The visual was used with such frequency that it became a "classic". It's popularity was attributed to the succinct depiction of the majority of the then known vulnerabilities within computer systems. A novice to the problem could quickly grasp the complexity from an observation of the single page visual.

The task force recommended security characteristics under a system of constraints. The U. S. Government classified defense information within a well defined and long established structure. From the computer point of view, it was desirable to modify these rules; however, to do so would be equivalent to tailoring the structure to fit the computer operation. The task force viewed this action to constitute an inappropriate recommendation. Obviously then, a constraint was that a secure computer system must be consonant with the security classification structure.

A second constraint, at least initially, was the assumption that the general tenets that existed in regard to the manual security control procedures would prevail. For example, the task force recommended that a secure computer system not only identify the user, but also that the user establish (prove) authenticity. Additionally, the user was asked to receipt for any and all classified information that was available through any type of terminal.

In the formation of its recommendations, the task force recognized the following general characteristics as desirable in a secure system.

The system should be <u>flexible</u>. Flexibility consisted of convenient mechanisms and procedures for maintaining the system under conditions of shifting job assignments, the issuance and withdrawal of clearances, changes in need-to-know parameters and the transfer of personnel from one duty assignment to another.

The system should be <u>responsive</u> to changing operational

conditions, particularly in time of emergency. While not an aspect of security control per se, it was important that the system be responsive in that it does not deny service completely to any class of users as the total system load increases. The task force believed it was desirable to design special emergency features into the system which could suspend or modify security controls, impose special restrictions, grant broad access privileges to designated individuals and facilitate rapid change of security parameters.

The system should be auditable. It must provide records to the security control supervisor, so that system performance, security safeguards and user activities can be monitored. This implied that both manual and automatic monitoring facilities were desirable.

The system should be reliable from a security point of view. It ought to be fail safe in the sense that if the system cannot fulfill its security controls it will withhold information from those users about which it is uncertain, but ideally will continue to provide service to verified users. A fallback and independent set of security safeguards must be available to function and to provide the best level of security possible under the degraded conditions if the system is to continue operation.

The system should be manageable from the point of view of security control. The system should be supplemented by the capability to make appropriate modifications in the operational status of the system in the event of catastrophic system failure, degradation of performance, change in workload or conditions of crisis.

The system should be adaptable so that security controls can be adjusted to reflect changes in the classification and sensitivity of the files, operations and needs of the local installation. There should be a convenient mechanism whereby special security controls needed by a particualr user can be embedded easily in the system. Thus, the security control problem ideally must be solved with generality and economy. It would be too costly to treat each installation as an individual instance and to conceive an appropriate set of unique safeguards.

The system must be dependable; it must not deny service to users. In times of crisis or urgent need, the system must be self-protecting in that it rejects efforts to capture it and thus make it unavailable to legitimate users. This point bears on the number and kinds of internal records which the system must keep and implies that some form of rationing algorithm must be incorporated so that a penetration would capture at most a specified share of system capability.

The system must automatically assure configuration integrity. It must self test, violate its own safeguards deliberately, attempt illegal operations, monitor communications continuity, monitor user actions, all on a short time basis.

The task force identified some uncertainties. There are several aspects of secure computer systems which were impractical or impossible to assess at the time.

Failure Prediction. The state of computer technology was impossible to completely assess, much less specify, all hardware failure modes, all software design errors or omissions and most seriously, all failure modes in which hardware malfunctions lead to software malfunctions. The exisiting commercial machines had only a minimum of redundancy and error checking circuits and thus for most military applications there was unsatisfactory hardware facilities to assist in the control of hardware and software malfunctions. Furthermore, in the then present state of knowledge, it was very difficult to predict the probability of failure of complex hardware and software configurations; thus, redundancy was an important design concept.

Risk Level. It was very difficult to arrive at an overall probability of accidental divulgence of classified information in a security controlling system because failure modes and their probability of occurrence could not be completely cataloged or stated. Therefore, it was difficult to make a quantitative measurement of the security risk level of such a system. Also, it was difficult to design to some a priori absolute and demonstrable security risk level. Since the security risk probabilities of manual systems were not well known, it was difficult to determine whether a given design for a secure computer system would do as well as or better than a corresponding manual arrangement.

Computer systems differed widely in the capabilities that were available to the user. In the most sophisticated and highest security risk case, a user could construct new programs and new programming languages from the console and embed such new languages into the computer system for use. In such a computer system, offering the broadest capability to the user, the security problems and risks were considered the most acute.

It was observed that not only did many installations operate in the broadest capability sense but they also had an operational need to accomodate the cleared and uncleared users. The uncleared user operated under a minimum of administrative control. The uncleared user worked with unclassified data through physically unprotected terminals connected to unprotected communications lines. On the other hand, the cleared users operated with classified information through appropriately protected terminals and communications links.

The task force cautioned that it was unwise to attempt to accomodate both classes of users simultaneously. Although, they recognized that many installations had an operational need to serve both the uncleared and cleared users.

Cost. Unfortunately, it was not easy to estimate the cost of security controls in a computer system. Very few computer

systems were in operation that attempted to provide service to a broad base of users working with classified information.

The task force made policy recommendations which were intended to provide a security skeleton around which a specific secure computer system could be built. Additionally, there were recommendations that set forth the responsibilities and functions of the personnel needed to evaluate, supervise, and operate a secure system. The task force recognized that this was a new field and their work represented the first major attempt to codify the principles.

The means to achieve system security objectives were based on any combination of software, hardware and procedural measures sufficient to assure suitable protection for all classification categories resident in the system.

The task force recommended to the maximum extent possible that the policies and procedures incorporated to acheive system security should be unclassified. However, they did point out that specific keys, passwords, authentication words and specifically sensitive procedures required classification.

The task force stipulated a number of system personnel to be responsible for security. For the first time the burgeoning computer security field was provided with job descriptors that defined the responsibility for the integrity of data processing. Depending upon the nature of the installation, some or all of the following categories of personnel would be associated with the system.

* **Responsible Authority.** The head of the department or agency responsible for the proper operation of the secured computer system.

* **System Administrator.** An individual designated as responsible for the overall management of all system resources, both the physical resources of the system and the personnel assigned to it.

* **System Certifier.** An individual designated by an appropriate authority to verify and certify that the security measures of a given computer system and of its operation meet all applicable and current criteria for the handling of classified information. The system certifier would also establish the maximum security level at which a system and each of its parts could operate.

* **System Security Officer.** An individual designated by a Responsible Authority as specifically responsible for (1) proper verification of personnel clearances and information access authorizations; (2) determination of operational system security status to include terminals; (3) surveillance and maintenance of system security; (4) insertion of security parameters into the

computing system; and (5) security assurance.

* System Maintenance Personnel. The individuals designated as responsible for the technical maintenance of those hardware and software system features which (1) must operate with very high reliability in order to maintain system integrity with respect to security matters, and (2) maintain the basic functioning of the system.

* System Operators. Those personnel responsible for performing the manual procedures necessary to provide and maintain on-going service operations of the system.

Finally, the task force focused on the user. The user was required, by system administration policy, to have sufficient identity within the system in order to be provided authorized access to all requested material, but no more! The user was required to identify and authenticate their identity to the system when the system requested it. The System Security Officer was responsible for the design of the authentication techniques.

A properly authenticated user was responsible for all action at a given terminal between the time that the identity had been established and verified and interaction with the system was terminated and acknowledged. Termination could occur because the user notified the system of departure or because the system suspended further operation with the user. The user was responsible for observing all designated procedures and for insuring against observation of classified material by persons not cleared for access to it.

The task force called for a program of continued research into encryption techniques and devices. It was essential in order to maintain separation between cleared and uncleared users. In fact, a whole array of research programs were advocated. A research program that would model a comprehensive automatic monitor for security controls and more reliable self checking hardware architectures. A research program that explored the methodolgy for identifying the failure modes and accurate predictions of failure probabilities. A research program into the certification procedures for esatblishing a secure system for processing classified information. Also, a recertification procedure for the system when it underwent hardware and/or software changes. Finally, a research program into the design of new machine architectures where the security controls minimally affect the efficiency or cost of the new system.

On 5 January 1970, Ware forwarded the Study Report of the Task Force on Computer Security to the Defense Science Board. He informed the Board that this effort was the very first attempt to codify the principles and details of a very involved technical-administrative problem. The effort reflected the best ideas of individuals knowledgeable about a problem that was relatively new and has not been solved in the breadth of scope defined by the task

force. There was no significant difference of opinion within the task force on the general content of their effort. Some aspects of the problem were so new that there was a difference of opinion on a few subtle details.

The Report was circulated within the Security Communications organization for comment. The communications security staff opined that the study was intended to provide broad, general guidelines, not necessarily applicable to any selected computer system. As such, even though the report was several months in preparation, the report was still considered current and factual. Among the important factors in the deliberations about the efficacy of the report was its usefulness at the national level. Thus, the Ware Report was considered a useful input to the committee being established as the result of the recent United States Communications Security Board recognition of the computer security problem.

Upon publication of the document, the report assumed a classical character and became known as the "Ware report".

(b)(3) - 5 USC App. 4, Sec 207(a)(1)(2)
(b)(3) - 50 USC 403g Section 6 of the CIA Act of 1949
OGA

CHAPTER 5

THE INTELLIGENCE COMMUNITY "RESPONSE"

An intelligence community working group concerned with computer security was formally established in the spring of 1968. It was named the Computer Securtiy Subcommittee of the Security Committee of the United States Intelligence Board. Originally chaired by Central Intelligence Agency employee, [redacted] the Subcommittee was comprised of employees from the Security and Counterintelligence organizations within the various United States Intelligence agencies.

The following were the Subcommittee membership agencies:

Central Intelligence Agency

Atomic Energy Commission

Department of the Air Force

Department of the Army

Department of the Navy

Defense Intelligence Agency

Federal Bureau of Investigation

Department of State

National Security Agency

The NSA representation was provided by the Office of Security, M5. In fact, the M5 organization was heavily involved in the early activities of computer security. Initially, the M5 role in computer security began with a request from the NSA Community On-Line Intelligence System (COINS) network manager, Mr. George Hicken to appoint a Security Officer responsible for a new "experimental" network that will net computers throughout the U. S. Intelligence Community. The Security Officer responsibilities were to facilitate the secure transmission of SI intelligence through the community computers with a strict adherence to the principle of "need-to-know". This involved the breaking of new ground in security technology involving the networking of computers. Thus, M5 was presented a new challenge along with an opportunity to explore the new science of computers in the development of a different kind

of security. This was the first attempt, anywhere, to net diversified computers in an assortment of intelligence agencies without the benefit of computer standards or security standards.

The M5 role, on behalf of NSA, in the activities of the USIB computer security subcommittee, in many ways mirrored the internal avtivities of M5 in computer security within NSA. However, intially, M5 was disjointed in this activity, that is the computer security responsibilities of internal NSA and the external responsibilities were the responsibility of different offices within M5. Soon, it was realized that what was needed, was the establishment of a technical group to address the needs of computer security. So, in 1968, a technical security office was established, labelled M503, and given the mission to address the computer security and technical security problems.

The M503 organization was assigned the responbilities of NSA representation on the Computer Security Subcommittee and continued in that role until 1975. During the tenure of M5 many accomplishments were achieved and major policies were promulgated within the U.S. Intelligence community. Some of the more significant publications included: "Guidelines for ADP Diaster Prevention and Contingency Back-Up Planning", "Degaussing Procedures for Computer Storage Media" and "Guidelines for the Security Analysis, Testing and Evaluation of Resource Sharing Computer Systems". However, the most far reaching document that impacted upon intelligence community computer operations was the publication of the Director of Central Intelligence Directive No. 1/16, "Security of Compartmented Computer Operations" dated 7 January 1971. This document prescribed the minimum parameters necessary for member agencies to operate their computer systems when processing compartmented intelligence information.

The computer security subcommittee recieved most of its tasking from its' parent organization, the Security Committee. In fact, the intial tasking was to conduct an analysis of the security threat posed by the possibility of hostile exploitation of weak points in the computer operations of the Intelligence Community. This tasking was accomplished by a request that the Counterintelligence Staff of the Central Intelligence Agency report any known cases where hostile services had attempted to exploit the security vulnerabilities of U. S. computer operations. As a result, the Central Intelligence Agency, the Defense Intelligence Agency and the Federal Bureau of Investigation provided information on several cases involving hostile attempts to exploit personnel either associated with Community computer operations or employed by American computing manufacturers engaged in government operations.

Among the cases reported were the following:

1. The FBI controlled an operation which began in early 1969 in which the Soviets attempted to obtain intelligence information through a high ranking Air Force officer stationed at the National Security Agency. The Soviet targets covered varied

areas, including NSA computer operations. The officer's duties did not place him in direct contact with the NSA computer operations and no information in this area was furnished to the opposition.

2. In 1967, the Soviets attempted to recruit an employee of Minneapolis-Honeywell Corporation stationed abroad. The Soviets requested the American, a programmer, to provide them all information and data on his company's computers. In exchange the Soviets offered to finance the American in his own business.

3. DIA provided information on an illegal attempt by the Soviet Trade Mission in East Berlin and a known KGB officer to obtain a classified computer used in a United States missile weapons system. In the first quarter of 1966, a West German exporter met a Soviet delegation to discuss a contract for a shipment of cotton and textiles to the Soviet Union. During this meeting the KGB officer asked if the exporter could be enlisted in an effort to obtain an NDC 1051-A1 computer manufactured by North American Aviation. The exporter contacted North American Avaition and shortly thereafter received a visit from West German and American security officers who informed him that the computer was classified equipment employed in a U.S. missile weapons system. The exporter was advised not to undertake any further steps toward obtaining such a computer. Subsequently this exporter was in contact with a businessman in Barcelonia, Spain, familiar with Spanish Army procurement procedures, through whom the exporter was actually able to inspect such a computer at an American Air Force Base near Madrid and was given to understand that a purchase could be arranged. At that point the exporter decided that the risk was too great and negotiations ceased.

4. In September 1966, several Soviet representatives unsuccessfully attempted to steal the core memory hardware section of a computer displayed by an American firm at a computer exhibit in Moscow. Later two employees of the company were offered monetary bribes if they would provide the Soviets with the core memory. As a result, company employees disconnected the core memory section each evening and stored it for safekeeping. Later, when leaving the country, company officials personally carried the core memory through Soviet customs.

(b) (1)
OGA

5. CIA reported an incident

(b) (1)
OGA

[redacted]

6. The Atomic Energy Commission reported an incident regarding a technique which could permit the accidental or intentional disclosure of classified data to unauthorized personnel through by-passing the storage protection feature of main memory. This deficiency was accidentally detected while checking out a scientific computer program on an IBM 360/50 using OS/MVT (operating system 360 which performs multiprogramming with a vairable number of tasks). Later, discussion with IBM revealed that all IBM 360 computer systems operating under the control of Disc Operating System (DOS), Tape Operating System (TOS), Basic Operating System (BOS), Basic Programming System (BPS) and Operating System (OS/360) are vulnerable to this technique. This deficiency can be corrected by the fetch protection feature offered by IBM; however, fetch protection can be installed only on IBM models 360/50 and above.

7. On 14 April 1969, an article entitled " Magnetic EDP Tapes As Intelligence Targets" appeared in Der Spiegel.[12] The article explained that the International Business Machines (IBM) in Sindelfingen, Wurttemberg, again and again rewarded its engineer, Gerhard Prager, with money bonuses. Prager, who was employed in the claims section of an IBM affiliated plant as a data processing installations specialist, took care of customer complaints on a homework basis and figured out improvements on IBM computers.

In 1968, the 4th Senate of the Stuttgart Senior Provincial Court sentenced the very active mechanic to two years in prison. Prager had been an agent of a GDR spy organization called the HVA (Main Administration for Information) in the East Berlin Mfs (Ministry of State Security). The trial of the Mfs agent disclosed a hitherto unknown game played by Eastern Intelligence in West German industrial enterprises: computer espionage.

At a computer center, IBM had stored data on planning, production, personnel and profits of 3,000 West German industrial enterprises on magnetic tapes and processed these data on a contract basis. Eastern agent Prager did overtime work, copying the tapes on duplicates, while IBM, not suspecting anything whatsoever, rewarded his enthusiastic work for the company with bonuses. Prager then sent the copies to the HVA in East Berlin.

---

[12]Article; Hamburg, Der Spiegel, German, Vol 23, No 16, 14 April 1969, p 95

In HVA the intelligence technicians had the IBM collection printed out on their own data processing machines. Programmers decoded the symbol and number combinations and finally translated them into legible report language that could be understood by the industrial analyst of HVA.

The data on the personnel of the 3,000 West German industrial enterprises were then part of the HVA data base. In these documents, the East Berlin espionage headquarters was able to look for potential agents for industrial espionage in West Germany.

The details on the planning, production and sales of the enterprises for whom IBM handled the data processing were turned over by the HVA to the pertinent ministries of the chemical industry, the light industry and the heavy machine building industry. The ministrial planning bureaucracy again passed the information on to the corresponding GDR government agencies for further utilization.

This method definitely proved to have a future. Of course, computer espionage, which was opertionally carried out by Mfs agent Prager was still a rather young branch of the intelligence business. According to one West German cyberneticist, "the spy of the seventies will no longer come in from out of the cold; by that time, he will bring hot EDP (electronic data processing) programs."

Engineers and counterintelligence had not yet figured out effective protection for computer-stored information. But even then, the HVA in East Berlin did not exclusively depend on the supply of stolen data on tapes or disks that were smuggled to it.

Telephone lines could also be tapped for the illegal recording of computer cables. Saboteurs could even feed the computers misleading information from their end and thus infiltrate false data into industrial programs.

East Berlin's espionage chief, Major General Markus J. Wolf, head of the HVA, recognized the possibilities of computer espionage in West German industry, science, technology and research already at a time when the GDR itself only had a few data processing installations. Five years prior (1964), he ordered a long-range plan to be worked out for this particular espionage operation. One of the first engineers who joined the East Berlin intelligence outfit for this purpose was Gerhard Prager.

In the GDR, Prager first of all was given basic computer training and was then assigned the job of obtaining further training in the data processing industry in West Germany. Finally he was ready to obtain a key position for the HVA in the East by getting a job as a specialist in the West.

This crack agent supplied not only taped information; he also informed the HVA as to which IBM models worked perfectly.

Only after receiving this information did East Berlin's agent for East-West German trade, Heinz Behrendt, order the proper IBM machines through trade.

And so the secrets of West German industry were decoded in East Berlin -- on West German computers.

It is interesting to note that at the time this study was conducted no information was developed indicating that there had been any technical penetrations of Community computer operations by hostile services. The reports received through several USIB agencies reflected examples of hostile attempts to recruit, as agents, personnel employed in or associated with the Intelligence Community and other computer operations.

Nevertheless, the conclusion of the Computer Security Subcommittee was that in the absence of stringent security measures, a hostile penetration of computer operations in the Intelligence Community was a real threat.

Surprisingly, there were benign threats, as the following illustrates!

As an adjunct to the threat study, a member of the M503 organization learned in conversation with the NSA IBM representative that as a matter of IBM commercial practice all IBM personnel were instructed to observe and record the types of competitor computers in service at IBM customer facilities. The IBM representative revealed that the Corporation recorded all this information in a central IBM computer at their Federal Systems Division headquarters. M5 requested a copy of this listing and learned that the majority of the computing power at NSA was recorded at the facility. NSA had always classified its computing capability as Secret, and here at the IBM facility it was recorded as a matter of commercial competitive practice with no classification or security protection afforded the information other than IBM confidential, an inbred company proprietary practice. To further compound the situation, here along side the NSA account, was the CIA account with similar information about that organizations computing capability. An agreement was reached with IBM to disperse this information throughout the system.

The threat report reinforced the popular belief that computers needed security attention not only from malicious users intent on obstructing operations of computers but also from espionage and even possibly sabotage from foreign agents. The threat report was the foundation on which other efforts were initiated. It documented the hostile interest in computers as well as the vulnerabilities posed in the use of computer technology in the Intelligence Community.

Around the time of the threat study, another effort was published, entitled; Considerations on the Security of Files in the Presence of Multiple Access to Computers. This statement of concern

was expressed by the Research and Development Subcommittee of the Information Handling Committee (IHC), USIB. This effort, by the R&D group, reinforced the concerns of the intelligence community. It reiterated many of the vulnerabilities previously enumerated.

The R&D group did highlight a system weakness that received little attention in previous studies. The vulnerability was "spillage". It manifested itself by displaying information at the wrong place or the wrong time. It was not a new phenomena, but occurred numerous times in the past and thus continued to be a serious possibility with computers. The best laid plans must take into consideration a malfunction. This was particularly true with the development of computers where a lack of standards failed to develop. The introduction of new systems tended to degrade the established security structure. What was needed was a declaration as to the acceptable risk that was tolerable. For example, "spillage that occurred as often as one time in a hunder million was acceptable." The computer security subcommittee agreed with the findings and recommendations of the R&D subcommittee and embarked on a program of investigation.

There was need for a broad program of investigation into safeguarding of information in computer controlled files. A recommended starting point were the active systems in the community, for example COINS, RYE and ANSRS. The effective procedures developed on those systems could serve as the basis for further developments.

The subcommittee felt compeled to provide the community with a set of security standards that would provide a minimum of protection to the operational systems. They undertook the effort to write a document that was a Directive from the Director of Central Intelligence applicable to the entire intelligence community. It specifically addressed those resource sharing systems that processed "sensitive compartmented information". The term was defined to include all information and material bearing special community controls indicating restricted handling within collection programs and end products for which compartmentation was formally established.

The greatest concern on the part of most member agencies was that the document not inhibit the mission of their respective agencies by enacting directives that specified elements of security that were not attainable in the inventory of operational systems.

So, a practical approach was adopted by unanimous vote to insert the following paragraph in the publication of DCID 1/16.

> "The diversity and complexity of such computer systems now in place in the Community and those already designed for future placement may not provide for compliance with the requirements of this directive in their entirety. Recognizing both the validity of the requirements and the difficulty involved in their application to currently installed and already designed

systems, the extent to which the requirements of this directive are applied to such systems is left to the determination of each USIB member in view of his ultimate responsibility for the security of sensitive compartmented information."

Following on the heels of the publication of DCID 1/16, the Computer Security Subcommittee was charged with preparing the "Guidelines for the Security Analysis, Testing, and Evaluation of Resource-Sharing Computer Systems". This effort was promulgated at the urging of the Defense Intelligence Agency (DIA) member, who was anxious to accredit the Analyst Support and Research System (ANSRS) for multi-level security operations. The DIA requested the USIB to task the Security Committee to write the guidelines for the security testing of such systems. The USIB approved the request at their 12 May 1970 meeting. Subsequently, the Computer Security Subcommmittee found itself researching and writing the document with the technical assistance of computer specialist of the various member agencies. On the publication date, 7 April 1971, particular attention was brought to the non-prescriptive nature of the document. The emphasis of this fact was due to the majority feeling among the subcommitee membership that it was the responsibility of the independent member agency to conduct its' own security analysis and eventual accreditation of their system without USIB membership participation. However, as we will see later, DIA adopted the philosophy of testing the ANSRS with community participation. The invite to participate in the test effort was almost a challenge to attempt to subvert the security parameters structured within the system.

The subcommittee was endowed with zeal to seek solutions to the computer security problem. In their beginning, they were prolific in their publications of policy and guidance. But, by 1976, the bulk of their contributions to the subject were accomplished. They did, however, update some of the previous publications and in particular completed a re-write of DCID 1/16 and added a new section that addressed networking security. The Computer Security Subcommittee was to continue functioning as a USIB body until 1980, when re-organization and change in the Intelligence Community brought about its' demise. NSA remained involved to the very end.

Chapter 6

SUBVERTING THE DIA ON-LINE SYSTEM (DIAOLS)

Before we begin to tell the story of this unique event in the history of secure computing, clarification is in order about the DIA system. In 1969, the DIA system was known by the acronym ANSRS which was the ANalyst Support and Research System; in 1971 the name was changed to DIAOLS, the DIA On-Line System. The constant in this story was the hardware, the General Electric 635. The dynamic, as always, was the software. The event was unique because it was the only time that a general purpose computing system, in the intelligence community, was subjected to this kind of an approach in an attempt to acheive accreditation for "multi-level" operation.

The events unfold starting in August 1969 when the ANSRS Project Officer, Roy Morgan had informal discussion with the Chairman of the USIB Information Handling Committee (IHC), Robert Taylor. They talked about the prospects of using ANSRS as the medium for establishing operationally relevent and feasibile criteria, techniques and safeguards sufficient for multi-level security accreditation of shared-resource computer systems serving the intelligence community. It was generally acknowledged throughout the community that the achievement of muti-level security controls in such systems was necessary before the community could cost effectively exploit advanced ADP technology to anything near its full potential for intelligence applications. The conversations concluded with an agreement that the DIA ANSRS Project had achieved sufficient progress in the ADP security area to make this system a promising candidate for a controlled multi-level security test. Further, the IHC would consider sponsoring such a test.

The DIA believed, that with IHC sponsorship and community wide participation in the test, the following major benefits would be attained.

a. It would enable DIA to gain multi-level security accreditation for ANSRS. This would exploit the system's full potential much sooner than would be possible without the direct involvement of USIB authority.

b. ANSRS accreditation would provide practical guidelines

for the establishment of community wide general criteria to which shared resouce ADP communication systems must conform if they were to be accredited for muti-level security operations.

c. Community wide participation would cultivate in member Agencies the expertise necessary for evaluation of individual intelligence ADP systems. This would also facilitate the sharing of information on developing computer security techniques through formal and informal channels. It would also develop procedures for the expeditious accrediting or re-accrediting of specific computer systems when more than one USIB member agency was involved.

The DIA requested the IHC to coordinate as necessary with other USIB elements, particularly the Security Committee because of their active role in computer security. Contact with non-USIB agencies, especially those having an interest in data privacy matters and computer security were especially desired. DIA also requested permission to handle SI and TK special category intelligence data in addition to collateral data; this would establish a true muti-level environment. DIA requested to manage a working committee comprised of technical ADP, communications and security experts from across the intelligence community. They felt that the committee should conduct extensive probes of the technical, procedural and administrative safeguards in order to uncover any weaknesses and propose remedies. The committee, when satisfied, would recommend ANSRS for multi-level security accreditation.

As a follow up to the Committee efforts on ANSRS, the group would draft general criteria for multi-level security accreditation of intelligence data handling computers. Additionally, the committee would conduct periodic reviews of technological advancements and recommend appropriate changes to accreditation criteria when warranted.

The DIA described the environment, configuration and testing previously conducted on the ANSRS. The ANSRS security document authorized it to operate in a "quasi multi-level" mode. That was to say that the processing of collateral and Special Intelligence (SI) was permitted as long as the system was encompassed within SI secure boundaries.

ANSRS was subjected to test and evaluation and the results were as follows:

(1) Over 2.4 million individual tests of the computer's memory boundary protection and executive software protection features indicated no malfunctions occurred in these key hardware safeguards.

(2) Almost 220 thousand individual tests of System software indicated no failures in any of the System's primary software security safeguards.

The ANSRS Test and Evaluation Report concluded, "as a whole, the security safeguards provided for ANSRS have collectively provided adequate protection for all levels and categories of classified information handled by the System." Based on this conclusion, the recommendation was made that "efforts should be exerted to acquire multi-level security accreditation for ANSRS."

The DIA presented a description of the test environment in which the controlled multi-level security was envisioned. For the ANSRS test would involve two major expansions beyond the current operational mode.

First, a special category of TK data was placed in the system. Access to this data was only through remote terminals located in approved TK secure areas. Involuntary software controls prohibited TK data from routing to an unapproved terminal. This was aided by an access control ANSRS security software program based on individual identification and authentication.

Second, several remote terminals were designated for access to collateral material, only. However, physical access to the terminal required at a minimum a Top Secret clearance and the individual was eligible for access to SI and TK data. Again, the software individual identifier and authenticator remained in effect.

DIA was also in the process of revising security provisions based on improvements and recommendations presented in the Test and Evaluation Report as well as the experience gained since the system began operations in August 1969. In addition to retaining the basic technical, proceduarl and administrative safeguards; key changes for accomodating muti-level operations are described herewith.

Installation of a software control feature limited the transmission of particular levels and/or special categories of classified information to only specifically approved terminals. This new software had been available for only three months and was extensively tested during that time. Details of its operation and the summarized test results are discussed later in this chapter.

All ANSRS unencrypted communications lines, the computer facility and the main communications center were physically accredited for SI and TK traffic. All remote terminal lines were protected in accord with existing communications security regulations.

There were DIA elements that did not require access to special category data in ANSRS and they were provided collateral access via controlled access remote terminals. No SI and TK access was permitted.

DIA's assessment of the risk associated with the topography of the system was acceptable. They reasoned that should

a system malfunction occur, the detailed accounting and audit trails automatically recorded would enable detection. Thus, timely action would be taken to administer an inadvertent disclosure oath to the person or persons involved.

The recently completed ANSRS Test and Evaluation Report indicated that security safeguards dependent on ADP hardware and software had a very high reliability, particularly when their operation was closely monitored. Even though the test and evaluation was not intended to measure the comparative reliability of computers and human beings in performing data handling operations, the results strongly suggested that the probability of human error was substantially greater than that of computer hardware or software error. Thus, DIA judged that controlled muti-level security operations which depended on ADP hardware, software and communications features to compartment and control access to various classification levels and special categories of information was no riskier than existing manual systems for handling classified documents and "will, indeed, probably be less risky." This judgement was further reinforced by the reliability statistics presented in the Test and Evaluation Report.

DIA expressed great confidence in their "extensive" accounting and auditing features and opined that "there is little likelihood" that any penetration attempt would go undetected. The TEMPEST problem presented no greater threat whether the system operated in single level mode or muti-level mode. This was so because ANSRS was physically and cryptographically protected in accordance with communications security features.

Under the single-level (also, known as the quasi multi-level mode) operations, the remote terminal user was not allowed to enter programs for direct execution by the system. There were only two capabilities available to remote users, the Intelligence Support System (ISS) and the BASIC interactive computation language and both operated strictly in an interpretive mode. This meant that users' commands to the system, in either case, were translated into pre-established sets of machine instructions which had already been thoroughly tested from operational and security perspectives. Since the user could not access the machine instructions directly, the user could not in any way modify them; nor could the user arrange to bypass the system's hardware and software security safeguards.

DIA addressed the impact of the test on the current operations as well as future development of the system. As an operational system, ANSRS provided daily support to intelligence analyst and managers in numerous DIA functional areas. Therefore, the conduct of the test was not permitted to impede the continuous support to operations.

As a dynamic system, ANSRS frequently underwent changes to increase reliability and responsiveness to the user. Additionally, expanded applications occurred in various DIA functional areas. The controlled muti-level test could not involve a "freeze" on such

development efforts during the duration of the test.

In accord with the Project ANSRS Implementation Plan, the DIA developed a greatly expanded software system based on the General Electric company's GECOS III (GEneral Comprehensive Operations Supervisor, Version III). It enabled the concurrent conventional batch, remote batch and interactive time-sharing operations. DIA did not want to shift to GECOS III until ANSRS was accredited for multi-level security operations with the general software configuration; i.e. the General Electric 635, Dartmouth, Time-Sharing System. DIA proposed additional testing to accredit for muti-level operations under the GECOS III based configuration after completion of its development.

Let us now turn to an understanding of the ANSRS remote terminal access control software, the composition of the testing methodology and the statistics produced as was previously mentioned.

Every data base file and BASIC computational program stored in ANSRS had a code associated with it which identified the overall security classification level and any special handling categories that applied to that file or program. At the same time, every ANSRS remote terminal was associated with a list of classification and special category codes which described the levels and special categories of data that it was cleared to handle. Whenever a user, successfully identified and authenticated himself/herself to the system at sign on time, attempted to access a file or BASIC program, the system software first checked to insure that the user was authorized access to that file or program. The software then performed a check to insure that the particular remote terminal through which the user was accessing the system was cleared to handle the classification level and special categories of information which that file or program contained. The classification/special category code associated with the particular file or program had to exactly match one of the codes contained in the list of codes associated with the terminal from which access was attempted. Otherwise, the system automatically denied access, recorded the denial in the system's activity log and notified the computer room operations staff via a message on the computer control console.

This software security check described above was performed not only when a user initially attempted to access a file or program, but also each time output from that file or program was directed to the user's remote terminal.

The ANSRS Test and Evaluation Report described techniques used to test the hardware and software security provisions of the system. Many of the tests, including all those conducted on a continous basis by the system's automatic security test program, had been continued and expanded since the conclusion of the formal ANSRS Test and Evaluation on 30 June 1969. Among the additional security checks incorporated into the automatic security test

program was one which tested the system's response to an attempt to access an SI data base file from a remote terminal channel which, for test purposes, was only authorized to access collateral files.

During the period 2 September through 28 November 1969, the automatic security test program conducted a total of 7,098,927 hardware checks dealing with memory boundary protection and executive software protection features. It also conducted a total of 645,357 software checks on the system's responses to various "legal" and "illegal" inputs. Of these software checks, 1,787 tested the system's response to an attempt to access an SI file with a user access code authorized to enter that file, but from a remote terminal channel not authorized to handle SI data. In 100 percent of the hardware and software checks listed above, the system's response indicated that the security safeguards were functioning properly.

In addition to the automatic security test programs, some testing was conducted personally by ANSRS users. The testing involved designating selected ANSRS remote terminals for limited collateral traffic only, although the terminals were located in approved SI areas. Software based restrictions were imposed and users attempted to access SI files. During the period 2 September through 28 Novemeber 1969, 241 such attempts were made without one success; all were rejected.

Well, with all of this impressive security testing data, DIA was now ready to formally approach the USIB and request member agency participation in the multi-level security testing of the ANSRS. The request was to be channeled through the sponsorship of the IHC. From the onset of this idea, there was opposition to it. The opposing view was concerned with establishing a precedent which could prove a significant burden on the IHC and other USIB committees in the event other agencies desired similar sponsorship. A better approach was advocated by an adherence to USIB approved and issued guidelines. Then the basic responsibility for test, evaluation and certification under said guidelines rest with the Agency seeking approval of their own system without formal USIB approval. Other agencies, as available, could assist in such efforts at their discretion. This then became the policy of the USIB.

Although the policy was established, the DIA was still anxious to have USIB member agency participation, believing that it would lend credibility to a successful test and evaluation of the ANSRS. After all, there was no known existing security problem with the system, the on-going testing efforts proved as much! DIA pursued the participation of member agencies in the Intelligence Community, finally winning acceptance, even from NSA.

In July 1971, the DIA announced to the community its' intention of conducting an analysis, test and evaluation of their DIAOLS computer network (formerly named ANSRS). The test teams were comprised of members from the Intelligence Community, the

Department of Defense and contractor firms. The teams were organized along functional areas of security, communications and automatic data processing. Members within each team were specialist in personnel security; physical security; procedural security; communications links; operational software; applications software: hardware and the general computer facilities commonly referred to as operations. With the teams established, the penetration tests were under way. The effort concludes in August 1972. For the DIA, the test was a disaster. The team effort proved that the DIAOLS was in an extreme state of vulnerability. The penetration of the GECOS system was so through that the penetrators were in control of it from a distant remote terminal.

In another instance an "agent" was able to penetrate the DIA computer building by counterfeiting a crude DIA badge and entered the facilities unchallenged by the guards. He was then able to obtain a Community On-Line Intelligence System (COINS) user's guide and make use of it at an authorized COINS terminal and was never challenged.

In January 1973, the IHC was briefed on the events involving the DIAOLS test and evaluation. They were also made aware of corrective measures employed by the DIA since the conduct of the test. The DIA improved their physical security posture by tightening the perimeter security; improved the security education program; and placed more controls on access to privileged terminals.

The CIA member expressed considerable skepticism about the probability of certifying any community network computer system as secure. System certification was an issue that must be addressed.

By 1974, the DIA was again soliciting the community for involvement in another mutilevel security test of the Defense Intelligence Agency On-Line System (DIAOLS), which was re-named from the ANSRS.

NSA declined to participate in that effort for a number of reasons. NSA felt that previous experience in software penetration studies, primarily GECOS, had led NSA to the conclusion that the failure of such an attempt was insufficient evidence for declaring a system secure. Therefore, while testing a system may indicate some of the risks associated with using that system in a given environment, failure to "break" that system cannot be the primary basis for certification for mutilevel operation. Rather, it was important to give adequate consideration to total system security.

The re-test never brought the desired results of mutilevel operations within the DIAOLS and it continued to operate in a system high mode, that being all places, people and things associated with the system must meet the security requirements of the highest level of intelligence information processed by the system.

CHAPTER 7

THE NSA ROLE IN COMPUTER SECURITY - REDEFINED

The activity described in the previous chapters, pursuaded the National Security Agency to take another look at the role it should play in computer security. In addition to these evolutionary events, there were constant urgings of senior level personnel within the Department of Defense and the Intelligence Community for NSA to assume a larger role. Additionally, there was a constant barage of door knocking at NSA by various people seeking answers to their computer security problems. This, in total, pursuaded the Agency to take, yet, another look.

On 17 May of 1973, eight years after the "invitation" to the conference at Santa Monica, California, an Agency senior level meeting with Dr. Tordella was held. The meeting on computer security resulted in a consensus that NSA's involvement in the field should be expanded and emphasized. It was decided to place the responsibility for managing the NSA computer security program with the Assistant Director for Communications Security (ADC). This action was also consistent with the charge from the United States Communications Security Board (USCSB) to develop a COMSEC Plan for computer systems. The following responsibilities for the ADC were enumerated.

* Act as executive manager for the NSA in computer security

* Establish and maintain in conjunction with other federal departments and agencies, a center of technical expertise on computer security which can selectively transfer information to any element of the Federal Government

* Develop or evaluate techniques and standards for computer security for the Federal Government

* Prepare policy recommendations on computer security for consideration by the Director, NSA, and through appropriate channels, the Director of Central Intelligence, the Assistant Secretary of Defense, Comptroller, and the Chairman, USCSB

* Ensure the effectiveness of NSA representation on National and DOD committees, boards, panels or working groups concerned with computer security

* Develop standards and techniques to assess the security vulnerabilities of computer systems used or planned for use by the Federal Government for processing classified data or other information requiring protection and determine the exploitation threat to such vulnerabilities

* In conjunction with the Assistant Director for Research and Development (ADRD), NSA, and acting within respective functional areas of responsibility, develop computer security technology to counter exploitation threats or to meet stated requirements of the Federal Government

* Through the National Bureau of Standards and in conjunction with the ADRD and Assistant Director for Production (ADP), assist in the evaluation of computer security techniques embodying cryptologic principles either developed or proposed for commercial non-Federal Government purposes

* In conjunction with ADP, evaluate proposals for the export or release to foreign governments of commercial or government developed computer security systems, technology or principles and make recommendations to the USCSB or other appropriate authority

After defining the responsibilities of this new organization, a definition for computer security was offered. It was defined as, "the protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquistion, manipulation, modification, or loss of information contained in the computer system or to prevent introduction of unauthorized information into the system."[11] In the definition, physical security was implied, however, it only applied to NSA operated computer systems and that aspect of COMSEC applicable to ADP or telecommunications systems.

With regard to the NSA role conflicting with the respective responsibilities of the ASD(C), ASD(T), the USCSB and the USIB, there was overlap, however it was the view of the NSA principals that it would not cause any serious problems.

In order to implement this new role, the ADC approved the establishment of a new division, S46, managed by Mr. James Tippett. S46 served as the focal point for S operations in the computer security field. Also, it provided the NSA representation on the Computer Security Subcommittee of the USIB and the ADP System Security Subcommittee of the DOD ADP Policy Committee. In

---

[11] Memorandum from S04 to D4, Subject: Computer Security, dated 15 June 1973

conjunction with the R&D organization of NSA, S46 initated its' mission by compiling a list of computer security issues that needed to be addressed.

From a philosophical perspective, if the DOD and the Intelligence Community could dedicate computer systems to individual problems, then the security problem could be reduced to the standard physical and personnel security practices. However, it was not practical to do this! Shared systems produced economies of scale which were attractive. Even more to the point, shared systems permitted a desired sharing of data. When this happened, the potential for undesired sharing was the obvious consequence. To this end, the R&D organization and S46 compiled a list of NSA computer security efforts as well as external activities involved in securing or addressing the security problems of systems. This then became the laundry list regarding issues to be addressed by NSA in its' new role as a provider of computer security needs. Lets look at a synopsis of the systems and problems that were addressed in the latter part of the 1960's and into the early 1970's.

The first effort we have previously addressed at length, the computer security techniques at NSA. It was conducted under contract to the James P. Anderson Company. The report, completed in April 1969, explained the computer security aspects of five different multiple user computer systems used in the intelligence community. A list of basic requirements for secure handling of classified information in a computer system was developed and the report concluded that a computer system could be built where the risks of disclosure of classified information were outweighed by the benefits of multi-level, multi-user operation.

Another contracted James P. Anderson Company study entitled "Methods for Protecting Files" was completed in June 1971. It focused on the feasibility of enciphering files in a computer system to minimize the effects of having files stolen and to aid separation of users on a need-to-know basis. An inverted file structure was used as a model and FORTRAN subroutines were coded and tested to assess the problems of key mapping, key management and relative enciphering/deciphering speeds. The report concluded that file encipherment offered a significant improvement in the protection of files stored in a multi-user computer system. The major disadvantage noted was a 10 to 20 percent increase in overhead necessary when the central processor was used to generate the key.

There existed an Air Force Security Technology Panel of which the NSA R&D and COMSEC organizations were participants. An Air Force R&D plan called for achieving effective computer security techniques in resource sharing systems. Of interest to the NSA was an R&D project which had a goal of producing terminal cryptos and cryptomultiplexing at the computer end. Additionally, research in file encryption and authentication schemes were also of interest.

The Advanced Research Project Agency (ARPA) network was a

distributive network interconnecting various computer systems located on university campuses. A few U.S. Government agencies participated to a limited degree. The control of the flow of information throughout the network was achieved through a computer known as an intermediate message processor (IMP). In 1971, ARPA officially requested NSA to study the design for a crytographic capability for securing the network on a host to host basis, the IMPs would be located in non-secure areas.

The NSA participation in the security assessment of the DIA ANSRS proved useful in providing insight into the weaknesses of the computer, the GE 635 using the GCOS III operating system. Other such test were contemplated, particularly systems using similar or like hardware and software such as the World Wide Military Command and Control System (WWMCCS) ADP system.

The LOGOS was an ARPA sponsored and NSA monitored contract conducted at Case Western Reserve University. It involved a "top-down" design system with interactive capabilities for the designer. The system permitted construction of computer systems, the operation of which could be completely tested and certified. This capability was viewed as a necessary step, although not complete, for construction of secure computer systems.

Stanford University had received support, indirectly, for work on program verification. Approximately, $400,000 was provided to the University under a program called BABBAGE. The work aimed at formal techniques for specifying and developing programs such that it was possible to prove that the program satisfied the formal specifications. In other areas of program verification, the NSA expressed interest in techniques for proving that security specifications were implemented correctly.

The Community On-Line Intelligence System (COINS) required the incorporation of user authentication and file access control. The Digital Bellfield concept was considered for the COINS requirement. The approach was to have crypto control computers (CCC) provide cryptovariables for a terminal file processor link only after it had authenticated the terminal and the terminal user. File access requests were also authorized by the CCC's. The CCC would perform these checks through the use of stored information about the users and their permitted access. This approach designated the responsibility of terminal and user identification and authentication to the user's local CCC and access control to the CCC local to the requested file processor.

As for the military services activiely seeking solutions to the computer security problems, the Air Force at Electronic Systems Command (ESD) was exploring a technique for user terminal authentication employing a credit card device.

The Navy was exploring the feasibility of separation of users in a data base.

The Army had not yet initiated a research program.

The Defense Communications Agency (DCA) managed the Automatic Digital Network (AUTODIN), a computer switched, communications facility. This was a transaction-oriented system that posed no vulnerability to the users (message originators and receivers).

The Joint Technical Support Activity (JTSA) of the DCA conducted a study and test of the Honeywell Information System, a series of computers that were procured for the World Wide Military Comand and Control System (WWMCCS). Although, this system with GCOS III system software was tested in the DIAOLS test effort, Honeywell was determined to make significant modifications to improve its security. The effort involved determining the weaknesses in the system which permitted an unauthorized user to access privileged information; operate in master mode; deny service by "crashing" the system and deny service by monopolizing the system. The results of the effort were to identify implementation versus design weaknesses; the results were to make simple fixes or major redesign in order to meet the specifications defined by the program manager. NSA participated in this effort.

On the commercial front, the International Business Machines (IBM) corporation expended considerable effort into the analysis of physical security problems related to computer systems. The effort resulted in the publication of a physical security manual for protecting systems. The manual also touched on the subject of detecting and controlling emissions. Also, at the IBM research facility there was an effort in the development of a cryptographic hardware device and a very small effort in program verification. At the IBM, Federal Systems Division, in Gaithersburg, Maryland, a considerable effort was expended to develop the Resource Sharing System (RSS). It was overlord on the release 18 of OS-360. RSS placed access controls on pre-defined files, implemented "fetch protect" and granted access under the direction of a system security officer. This work was orginally accomplished for part of the WWMCCS contractual bid and later became the basis of the first phase of a $40M expenditure by IBM in computer security..

As for the UNIVAC corporation, very little was accomplished outside of a small effort to improve the EXEC-8 operating system for the 1108 machine. It was part of the WWMCCS contract bid.

At the Control Data Corporation (CDC), the STAR, a virtual memory machine, had some potential for security. The General Motors Corporation, as a user, had written their own operating system. They attempted to exploit the virtual memory concept and some of the hardware features that provided for private and sharable data sets.

At the Honeywell corporation, their announced work was

limited to the Multiplexed Information and Computing Service (MULTICS). A discussion of this effort appears below under University work.

On the University front, there was development of a general purpose computer system at MIT and the Honeywell Information systems group of the Honeywell Corporation. The system was named MULTICS and was implemented on a Honeywell 645 computer. It was designed to operate as a general purpose computing utility. They designed the system so that a user could pay for any of the necessary resources needed to perform the job. The user could also control the sharing of the information and the system accomodated the protection of this feature. Additional security features allowed the user to link to other user's programs and data or change the base of operation to another directory with the other user's permission. The system could also revoke any access priviledges at any time. It was built on a virtual memory concept where segements of information were manipulated and protected by the system. MIT also received a new computer with hardware rings of protection for the system and its subsystem. It was noted as the most secure system of the times.

At Cornell University an interesting student record method, for handling those records, was developed. The system was designed around the use of passwords that allowed individual access and also provided a base for decipherment of the fields of files to which the user was entitled. The user had the program compiled, run and obliterated at the conclusion of the work day.

S46 basically pursued these efforts and provided representation on the USIB and DOD Computer Security Subcommittees. The DOD Computer Security Subcommittee raised the issue about the void that existed by not having a central technical capability as specified in the DOD Directive 5200.28. They recommended that the issue needed to be addressed.

In November 1974, Assistant Secretary of Defense, Terence E. McClary, sent a memorandum to the various departments and defense agencies concerning the subject of the DOD ADP Security Program. He cited the DOD Directive 5200.28, dated December 18, 1972, that outlined a comprehensive ADP security program for the Department. Although many of the elements of the directive had been successfully implemented, he particularly cited the lack of implementation to establish a central technical capability. The 5200.28 Directive defined the general role of this capability as assisting and advising DOD components in ADP system security testing. It would also assess the progress in the development and installation of secure systems.

As a result of McClary's office working with several DOD component representatives for several months, a validated list of functions was developed for the central technical capability. The list included the following:

1. Identification and coordination of R&D and operational projects aimed at solving ADP security problems.

2. The development of standard methods that assisted Defense Components in evaluating the security of their ADP systems.

3. Prepared guidelines in analytic techniques that strengthened the application of cost risk and cost effectiveness in the application of ADP security.

4. Provide a clearinghouse function for the exchange of technical information on ADP security.

5. Participate in national efforts to develop standards and criteria for ADP security.

The receipients of the memorandum were asked to provide formal comments and recommendations by December 20, 1974. The NSA response to this memorandum was positive as to the role that the Agency should play. Lew Allen, Jr. LTGEN, USAF, DIRNSA, pointed out that the subject of ADP security was closely related to COMSEC. In fact, it was projected that 80% of the computers used in the DOD in 1980 would be on-line, implying that they would transmit via telecommunications. Many of the safeguards for privacy would be at least partially dependent upon cryptographic solutions. He pointed out that cryptographic techniques, no matter how employed, fall within the purview of COMSEC as stipulated in the National Security Council Communications Security Directive (NSCD) of 25 August 1968. This same Directive made NSA the central technical authority for COMSEC in the Federal Government. Given this background, Allen felt that it would be the optimum and most cost effective arrangement for the DOD to have the function of the Central Technical Capability for ADP security assigned to NSA and not fractionate the non-COMSEC aspects of the ADP security to another organization.

Allen's view of the magnitude and complexity of the ADP systems security problem in the DOD called for additional resources to carry out the responsibilities of the Central Technical Authority. He estimated the FY 1975 resources to be an additional 67 billets and $4,549,000 in funding. The resources were intended to be used in the following manner:

EFFORT	MANPOWER		CONTRACTS
	BILLETS	SALARY	
R/D	19	$209K	$660K
Security Concepts Evaluation	8	80K	-
TEMPEST and Reliability	8	80K	200K

System Security Analysis	10	100K	1000K
Hardware and Software Systems Applications	14	140K	430K
Perform service and provide guidance	8	80K	1570K
	67	$689K	$3860K

Allen intended to disperse these resources amongst the S46 division and the R&D organization.

The response from the DOD was not what NSA had anticipated. The Office of the Secretary of Defense, Director, Telecommunications and Command and Control Systems summarized the views of OASD(C) regarding the provisions of the 5200.28 Directive. The Directive provided for the delegation of ADP system security approval authority to each DOD Component. Each Component evaluated the ADP systems within their jurisdiction and determined whether or not the system was in compliance with DOD policy. The central technical capability was envisioned as an advisory role. It would assemble, maintain and disseminate technical information avaiable from inside and outside Government on representative types of ADP systems. The OASD(C) advised that resource constraints precluded the initiation of additional programs. The computer security advice from NSA would have to be accomplished within exisiting resources. In light of the resource constraints, further study and assessment was needed before any final decision was made about assignment of responsibility for the Central DOD technical advisory capability for ADP security.

~~SECRET~~

During the latter half of the 1970s, the DOD conducted many studies into how to handle the technical aspects of computer security. Also, it struggled with the assignment of a department or agency that should be assigned the responsibility. In the Fall of 1979, Mr. Steve Walker, former NSA employee, employed at the Office of Assistant Secretary of Defense, Commmand, Contol, Communications, and Intelligence (OASD C3I) suggested that an evaluation center be established as a program management office at NSA and that it report to OSD. He suggested that the evaluation center should be modeled like the COINS Project Management Office. This suggestion brought objections from other DOD components because they believed such a center would not be responsive and it would be administratively complex. Walker continued to pursue his idea, and in August 1980 he met with Bobby R. Inman, Vice Admiral, U. S. Navy, Director, NSA/Chief, CSS. Inman endorsed the idea of a PMO at NSA which he had heard about the previous autumn. In fact, Inman expected to see something about the center in the consolidated guidance, but it was silent. Thus, Inman expressed to

Walker that Dr. Gerald P. Dinneen, ASD C3I should be encouraged to suggest it to him.

On 3 September 1980, Dinneen corresponded with Inman and requested consideration be given to the concept of an evaluation center at NSA. Dinneen suggested that the center be organized as a Program Management Office reporting to an appropriate level at OSD. Inman sought the advice of his senior staff about the Dinneen suggestion. The concept of the center produced some controversy within NSA as to its composition. The model of the COINS PMO for the center was considered not to be a good idea. The success of the COINS PMO was attributed to George Hicken, the manager. However, there were many negatives associated with the project. It did not have good community support. The original concept was for each participating agency to contribute billets and assign their personnel to the project on a three year basis; this never happened. NSA funded the program and provided engineers and computer science personnel to build the network. Progress was very slow. The PMO reported to the ASD(C3I) who was the program manager. The PMO was housed at NSA because of the needed expertise to build the network. Eventually, the PMO obtained its' own staff, contracts and R&D projects, yet it was all funded with NSA monies. The conclusion was that although COINS was a precedent, the evaluation center should not be patterened after it. The evaluation center should get the full commitment of those who participate in it.

Inman negotiated the structure of the Computer Security Center with Dinneen. The Center's establishment was based on the understanding that it was an independent organization reporting to the Director, NSA. The composition involved the consolidation, within NSA, of all activities involved in external support to Computer Security. On January 1, 1981, the Director, NSA was assigned the responsibility for Computer Security Evaluation for the Department of Defense. In March 1981, Mr. George Cotter was appointed the first Director of the DOD Computer Security Center. Later, in the mid-1980's, the name was changed to the National Computer Security Center.

CHAPTER 8

NSA AND PUBLIC CRYPTOGRAPHY

The roots of cryptography run deep into the past centuries. However, one only has to look back to World War II inorder to trace the beginning of issues arising in public cryptography. The war caused the U.S. Government to support many researchers in cryptology. One of those researchers was Dr. Claude Shannon of Bell Laboratories. His research led him to the development of a new branch of mathematics named Information Theory. His major work was published in 1948 and the following year he prepared a treatise on secrecy systems that applied information theory to cryptology. Since that time, cryptography has been a legitimate academic subject.

Shannon's work was very theoretical and dealt with the broad principles governing cryptography. He was not concerned with the finite details which comprise the tools of contemporary cryptologist. Consequently, most academic efforts in unclassified cryptography were of a theoretical interest with little practical value.

The 1950s brought the beginnings of the technological revolution that transformed the computer from an exclusive tool for science to a tool for business. By the mid-1960s, security weaknesses in remote timeshared computer systems were becoming apparent. Some of the weaknesses could be overcome by cryptography and that led to an ever increasing industrial investment into cryptographic research. The academic community would not be far behind.

A prime example of industrial cryptologic research was the work performed at International Business Machines (IBM). In the late sixties, the company decided to embark on studies involving cryptology. It was part of an overall program in data security that was initiated by IBM President, Thomas Watson, Jr. He believed that data communications was an up and coming thing and, historically, encryption had been the only way to assure the security of data transmissions. Watson's decision resulted in IBM establishing a cryptologic research group at its laboratory in Yorktown Heights, New York. The group. led by Horst Feistel, developed a cryptographic algorithm, which was given the code name, Lucifer.

In 1971, IBM was asked to quote on a special product for Lloyd's Bank in England. The product was for a cash dispensing terminal that included a device to prevent spoofing. IBM chose to

meet the protection aspects of the requirement by developing a version of its Lucifer crypto-algorithm for the terminal. With the development of the cipher, the research group concluded its work.

IBM then formed a group to develop data encryption products based on the Lucifer algorithm. The company chose, from its ranks, Walter Tuchman, a holder of a PhD in information theory from Syracuse University, to lead the group. He assembled the data security products group that included IBM employee, Carl Meyer, an electrical engineer with a PhD in electromagnetic theory from the University of Pennsylvania. By the end of 1971, it had become clear to Tuchman and Meyer that the Lucifier algorithm would not be strong enough in its original form for general purpose use. The Lucifer cipher was adequate for the Lloyds cash issuing system where a coded system prevented customer passwords printed on ID cards from being read and misused. However, the system would not withstand intensive cryptanalytic attacks over a period of time.

Consequently, Tuchman and Meyer spent the next two years ('72-'74) working to strengthen the Lucifier cipher. At the same time they subjected their improvements to "validation". They had cryptanalytic experts try and find flaws in the algorithim that would enable an attacker to crack it.

After completing their work, convinced of a strong product, they began to develop products based upon the algorithm. The products included the model 3845 data encryption device, a desktop unit intended to operate at the ends of a data communications link between a modem and a terminal or a modem and a computer. The model 3846 was a rack mounted version of the 3845. The group also developed the Cryptographic Subsystem, a hardware and software data encryption system intended to be used on large multi-terminal 370 systems to protect data transmissions and on-line files.

ENTER THE NATIONAL BUREAU OF STANDARDS (NBS)

In 1965, the Brooks Act was passed into law and it gave the NBS the responsibility to create standards which governed the purchase and use of computers for the federal government. Then, in 1974, a national concern with individual privacy prompted the Congress to enact the Privacy Act of 1974. This act was an attempt to keep confidential and secure all data on U.S. citizens that was in the possession of the U.S. Government. The two pieces of legislation fostered the notion of a federal standard for use in the U.S. Government that would protect unclassiifed data stored and transmitted by computer.

In 1968, the Institute for Computer Science and Technology, at NBS initiated several studies assessing the need for computer security. The results convinced the NBS to encourage the

development and establish a government wide standard for encryption devices. NBS was convinced that the best encryption method was the use of an algorithm.

In May 1973, NBS issued a solicitation through the Federal Register that encouraged interested developers to submit possible algorithms for consideration as the Data Encryption Standard (DES). The solicitation evoked very few responses and a second solicitation was issued in August 1974. IBM responded with their LUCIFER.

NBS knew of the NSA experience and expertise in cryptology. As a result, NSA was contacted and asked to assist in evaluating the quality of a DES algorithm. NSA responded in the affirmative and in consultation with NBS judged the IBM algorithm to be the best of those submitted. It would become the government DES.

However, before the official announcement could take place, private computer scientist and engineers, who had been developing their own encryption schemes, expresssed concern about the strength of the LUCIFER algorithm and the process through which the IBM product was chosen. The role of NSA was highly suspect. The critics looked upon this DES activity with distrust, suspicion and intrigue. Afterall, they reasoned, this involved the actions of a "super secret" intelligence agency whose business was to monitor the telecommunications of the world. Also, IBM refused to reveal the design criteria that was developed for selecting the strong substitution, permutation and key scheduling functions. In fact, they had been classified at the request of NSA. Futhermore, NSA suggested that the key size of Lucifer be reduced from 64 bits, the scheme submitted to NBS, to 56 bits (careful reading was required to discover that 8 bits of the 64 bit scheme were used as parity checks).

On March 17, 1975, almost two years following the first solicitation, NBS published two notices in the Federal Register. First, the proposed "Encryption Algorithm for Computer Data Protection" was published in its entirety. NBS stated that it satisfied the primary technical requirements for the algorithm of a Data Encryption Standard. The second notice contained a statement by IBM that it would grant the requested nonexclusive, royalty-free licenses provided that the Department of Commerce established the Data Encryption Standard by September 1, 1976.

On August 1, 1975, another notice was published by NBS in the Federal Register. It proposed a Federal Information Processing Data Encryption Standard. The notice requested from Federal agencies and the public comments regarding the proposed standard. On October 22, 1975, Dr. Martin Hellman, professor at Stanford University, and graduate student Whitfield Diffie, responded to the proposed standard in correspondence to the NBS. Hellman told the NBS that he and Diffie were concerned that, although the algorithm was probably secure against commercial assault, it was extremely

vulnerable to attack by an intelligence organization. He outlined a "brute force" attack on the proposed algorithm, using a special purpose parallel computer using one million chips to try one million keys each per second. He estimated the cost to build such a machine at 20 million dollars.

The NBS was concerned with adequate protection that was to be provided by the DES, therefore it continued to evaluate the algorithm and examined alternatives to issuing the standard. Hellman and Diffie felt they were largely ignored by NBS. As a result, and in order to get a wider hearing, they published an open letter in the Communications of the ACM (Association for Computing Machinery) in early 1976. They continued their assault on DES and maintained that it was weak due to the brevity of the key length at 56 bits. They suggested that the key length be increased to 64 bits and if possible to 128 bits, as was the case with the original LUCIFER scheme. They even turned to David Kahn, author and editor, and pursuaded him to write an article for the Op-Ed page of the New York Times, published on April 3, 1976. Kahn's article basically supported the position of Hellman and Diffie.

All of this publicity caused somewhat of an uproar, and finally, pursuaded the NBS to accept the fact that there was such a thing as cryptanalysis and that the Hellman-Diffie questions had to be answered. NBS chose a workshop format to address the critics. The first was held on August 30, 1976 and the attendees were mainly hardware specialist. The conclusion drawn at this worshop was that the Hellman-Diffie scheme was not implementable mainly because of the mutimillion dollar investment required. However, it should be noted that many of the participants at the workshop had vested financial interest in the DES scheme. They represented manufacturers who had started development and were reluctant to make changes.

The second workshop was attended mostly by software experts who had no financial interest in the project. They came to no consensus but did point out that the key length provided no safety margin. A detractor in the two worshops was the fact that the design principles used by IBM were classified and could not be revealed to the attendees. It made matters more difficult.

The workshops agreed, based on the information provided, that if DES were adopted it would be effective for little more than 10 years. The standard was adopted in early 1977 and became effective in July of that year. It was to be reviewed by NBS every 5 years.

The controversy surrounding cryptology was not to end with the adoption of DES. For in the same month that DES was to become effective, July 1977, public attention was again called to cryptology through a letter from Mr. Joseph A. Meyer, NSA employee, to Mr.E.K. Gannett, Secretary of the IEEE (Institute of Electrical and Electronics Engineers) Publications Board. The Meyer letter pointed to the possibility that some of the discussions and

publications of members of the IEEE's Information Theory Group could be in violation of U.S. export regulations relating to cryptanalytic equipment and information. Mr. Gannett circulated the letter amongst the members of the Information Theory Group. Copies of the letter were obtained by the press and stories began to appear alleging that Mr. Meyer was an employee of NSA and the intent of the letter was a form of NSA pressure directed toward the scientific community to defer from further activities that involved cryptologic research.

The press stories gave rise to additional allegations concerning NSA activities involving DES and cryptologic research. Some stories suggested that NSA had exerted pressure upon the National Science Foundation (NSF) to pursuade them not to fund grant proposals that supported cryptologic research.

All of this public attention did not go unnoticed at the U.S. Senate. The Senate Select Committee on Intelligence initiated an investigation. The investigation involved the following allegations:

1) NSA exerted pressure on the officials at NSF to withhold grant funds for scholastic research into public cryptograpghy and computer security.

2) NSA directed employee, Joseph A. Meyer, also a member of the IEEE, to write the letter warning the IEEE members that their actions involving cryptology could be in violation of export laws.

3) U.S. Government harassment brought on chilling effects in universities conducting cryptographic research, even to the point that one university withdrew its published material from the library shelves.

4) NSA while assisting NBS with the Data Encryption Standard "tampered" with the final algoritm in order to weaken it and thus create a "trapdoor" that only NSA could tap.

5) NSA forced IBM to compromise DES security by reducing the key size.

6) DES failed to allow for future technological advancements which would permit successful brute force attacks within several years.

The investigative results prompted the Senate Select Committee on Intelligence to conclude the following:

* NSA had not applied pressure on the NSF to prevent the issuance of grants for cryptologic research. However, some NSA officials expressed concern to NSF about certain grants with cryptologic ramifications. NSA was concerned about its ability to produce SIGINT and requested the NSF officials to permit NSA to be

involved in the review process of these proposals. The NSF agreed to NSA involvement in the review process and viewed NSA as the only location of competent cryptologic expertise in the federal government. However, NSF would not lessen its interest and willingness to fund good research proposals in this field.

* The investigation determined that Mr. Meyer's letter to the IEEE was intiated soley by Mr. Meyer. As a member of the IEEE, and knowlegable of cryptographic export laws, he was genuinely concerned about the activity of computer security and cryptography in the public sector. Mr. Meyer was not prompted by any NSA officials.

* There had been no government harassment of scientists working in the field of cryptography or computer security. The stories about a university withdrawing library material from their shelves had no basis in fact. However, it was noted by the senate committee that the novelty of public cryptology and the vagueness and ambiguity of federal regulations germaine to cryptology created an uncertainity which in itself was not conducive to creative scholarly pursuits.

* NSA convinced IBM that a smaller key size was adequate. The Agency indirectly assisted in the development of the S box structures. The structures were part of the algorithm that performed the iterative process. Also, NSA certified that the DES algorithm was, to the best of their knowledge, free of any statistical or mathematical weakness. NSA did not tamper with the design of the algorithm. It was the exclusive invention and design of the IBM Corporation. The only suggestion that IBM accepted from NSA was the key size. IBM was convinced that a 56 bit key size was more than adequate for commercial applications for which the DES was intended.

* The Intelligence Committee reported that an overwhelming majority of scientist consulted felt that the security afforded by the DES was quite adequate for a 5 to 10 year period in applications of unclassified information. It was especially noted that NSA had recommended that the Federal Reserve Board use the DES in their funds transfer system.

The Senate Intelligence Committee made several recommendations as a result of the investigation. The membership believed that because the subject was new to the public scene, it presented the potential for capriciousness in ambiguous and uncertain situations. Therefore, the committee recommended:

* that the appropriate committees of Congress should address the question of public cryptology by clarifying the role which the federal government should have in policies affecting public cryptology.

* that the NSF should decide what authorities and obligations it has to consider when national security implications

are involved in grant proposals.

* that NSF and NSA should initiate efforts to reduce the ambiguity and uncertainty which surrounds the granting of research funds for public cryptology.

* that NSA and NSF should discuss the need for NSA to become part of NSF's peer review process for the review of grant proposals for research in cryptography or cryptanalysis.

* that NBS should continue to follow developments in computer and related technology in order to be aware of any developments which could lessen the security of the DES.

DES GAINED ACCEPTANCE AND ENDURANCE

Hellman continued to badger the DES and his newer ideas approached effective cryptanalysis. Nevertheless, NBS and other supporters displayed little concern about such criticism. They pointed out that no scheme presented would cost less than 10 million dollars of investment in a special purpose computer to "bust" the DES. The popular view was that it was doubtless that anyone could read DES encrypted data, whether that would be the computer hacker or the most skilled embezzler. DES was widely accepted and was the only publicaly available cryptoalgorithm. Its acceptance was based on two reasons.

First, no one had demonstrated a fundamental weakness of the algorithm. The one serious proposal by Hellmann and Diffie to invoke exhaustive key testing until the correct key was found, was the method that designers of cryptoalgorithms hoped their adversaries would be forced to attempt. This method, given the key size was sufficiently large, would dissuade the attacker from attempting exhaustively testing the keys. If no easier attack on the algorithm was found, the algorithm designer succeeded in providing adquate security.

Secondly, acceptance of DES was based on the fact that the Federal Government endorsed it. There were no other algorithms with such an endorsement. Federal agencies were required to use DES for the safeguarding of unclassified information, but the private sector accepted DES because of the Government approved degree of security. Consequently, DES became the most utilized mechanism for the protection of unclassified data.

The Data Encryption Standard required that the algorithm be implemented in hardware for federal applications, but many corporations and individuals had programmed it in software. This method became so popular that the number of implementations was unknown. The popularity of the product hastened the production of DES based standards.

The American Bankers Association developed standards related to financial matters in both retail and wholesale banking. This meant that retail banking involved transactions between private individuals and a finacial institution, while wholesale banking involved transactions among financial institutions and corporate customers. Automatic teller machines identified the customer vis a vis a Personal Identification Number (PIN) presented by the customer at transaction time. DES was widely used in the protection of the PIN as well as preventing the alteration of the information used in the transaction. U.S. banks transferred in excess of 400 billion dollars daily and the Clearing House Interbank Payments System (CHIPS) processed 560,000 messgaes per week for a total dollar value of 1.5 trillion, DES was employed to protect these transactions.

The American National Standards Institute (ANSI) produced a Data Encryption Algorithm Modes of Operation Standard. Also, in the field of network security ANSI established a standard for information systems communications protocols at the transport and presentation layers of networks. There were standards developed for the management of PINs and standards for message authentication and key management.

The General Services Administration (GSA) was responsible for the promulgation of Federal procurement regulations. Prior to the passage of the Computer Security Act of 1987, GSA was responsible for the development of Federal Telecommunications Standards. GSA delegated this responsibility to the National Communications System (NCS) and they produced three DES based standards. 1) "Telecommunications: Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical and Data Link Layers of Data Communications, 2) "Telecommunications: General Security Requirements for Equipment using the Data Encryption Standard" and 3) "Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment".

As a Federal standard, the Federal Government established validation and certification programs for DES. This ensured product conformance in the use of DES. No other publicly available algorithm had been validated to this extent. DES has been validated as a secure algorithm every five years since it became a standard. It was recertified in December 1993. To the suprise of many and in particular those who claimed that the algorithm would remain secure for 5 to 10 years from its introduction, DES has endured for 20 years.

BEYOND DES

NSA continued to find itself immersed in controversy over public cryptography. This time the controversy revolved around the development of another cryptographic algorithm under development at the Massachusetts Institute of Technology (MIT). The event unfolds

At about the same time that DES was declared a standard. MIT professors Ronald Rivest, Adi Shamir and Leonard Adelman designed an algorithm that employed the use of public-secret keys to encrypt messages. The first way to employ the use of the algorithm was to enable a non-secret key to be used to encrypt a message that could be decrypted only by a particular secret key. Conversely, the second usage employed a secret key to encrypt a message that could be verified as coming from a specific sender by application of the sender's public key. This latter use of public-key technology was named a digital signature.

The algorithm attracted interest in the computer security field. Rivest planned to present the work at an IEEE conference in Ithaca, New York. However, our Argus-eyed defender of the secrets of cryptology again appeared on the scene. Mr Joseph Meyer, NSA employee, corresponded with the MIT authors and warned them that Soviet nationals would be present at the conference and publication of their algorithm was a potential violation of the International Traffic in Arms Regulation. The MIT professors were perplexed. They sought legal counsel and were advised to halt the dissemination of their work until the matter could be thoroughly reviewed. Officials at NSA were adivsed of the Meyer letter and promptly disavowed his correspondence. The paper was presented by Rivest and the whole issue of public cryptology was put to rest for the moment.

~~SECRET~~

Then, in the Summer of 1978, the issue resurfaces, only this time the challenge to academia was official. NSA requested a secrecy order with the patent office against a patent filing of Dr. George I. Davida, Professor at the University of Wisconsin, Milwaukee and graduate student David Wells. Davida and Wells had filed a patent application on a stream-cipher technique they had developed.

The application triggered a legal requirement of the Patent Security Group of the U.S. Patent Office to notify NSA of cryptographic inventions. The NSA responsibility was to determine if the invention contained subject matter that was classified and if marketed would be detrimental to the security of the United States. A copy of the patent was examined by the COMSEC organization (S) and the Operations organization (P). The S organization considered the invention unclassified but the P organization recommended that it be classified "SECRET". The P conclusion was based upon the advice of P1 that disclosure of the non-linear shift register features of the application could be detrimental to national security. The results were that the Commissioner of Patents and Trademarks issued a Secrecy order against the application. The order prohibited the inventor from marketing the invention. It was not well received back at the University of Wisconsin.

Werner A. Baum, chancellor of the University of Wisconsin's Milwaukee campus, decided to protest the action through the New York Times. On 31 May 1978, The New York Times reported that the University of Wisconsin was going to challenge the secrecy order imposed at the request of "a Defense Agency" on the University sponsored, publicly funded research on computer security. The following day (1 June) The Washington Post reported that the University of Wisconsin had asked the National Science Foundation to join them in appealing the secrecy order. And, on 2 June CBS evening news aired a brief interview with Davida in which he revealed that the University was considering legal action.

That very same day, 2 June, Howard Bremer, patent attorney for the Wisconsin Alumni Research Foundation, which filed the application for Davida, telephoned Lt. Col. Hougen, secretary of the Armed Services Patent Advisory Board and was asked for the name of the patent attorney for the " Defense Agency" that recommended the secrecy order. He was provided the name of John R. Utermohole, NSA patent attorney, who was contacted by Bremer. Utermohole explained to Bremer how secrecy orders worked.

All of the publicity alarms NSA Director, Bobby R. Inman, USN, who requested that the General Council obtain detailed information on the invention. Inman also called for a re-evaluation of the invention.

On 6 and 7 June NSA representatives from A, P, General Council, G, S, and NSA patent attorney office convened an evaluation committee that re-examined the Davida invention. On 6 June another event unfolded at the Commerce Department concerned with Davida. NSA General Council was informed that Commerce Secreatry Kreps was going to Wisconsin to say, inter alia, that the imposition of the Order was warranted. The General Council replied to Commerce that NSA was re-evaluating the matter and there was a possibility that the Order might be recinded.

On 7 June 1978 the NSA group reached a unanimous decision to rescind the order. A5 prepared the written correspondence to the General Council expressing that the secrecy order should not have been imposed.

All of this activity did not escape the attention of the Senate Select Committee for Intelligence (SSCI). On 8 June 1978, Stanley Taylor of the SSCI Staff asked the NSA General Council for all the information on the Davida case. The General Council explained how the Patent Secrecy Act operated. Taylor was unfamiliar with the procedure but had no critical reaction to it or the Davida case. Taylor was interested in the internal review process of NSA when a cryptographic invention was submitted to the patent office. The General Council told Taylor that NSA was reviewing its internal procedures with a view toward a more conservative approach.

On 19 June 1978, NSA issued a new regulation number 80-1

entitled, "Secrecy Orders in Patent Applications". This regulation required a more structured and stringent review under the direction of the General Council. All NSA conclusions required the signature of the Deputy Director or the Director.

In late December 1977, a patent application of Mr. Carl R. Nicolai of Seattle, Washington was referred to NSA for review. The invention achieved a novel and significant integration of various techniques in the spread spectrum area. The application was referred to NSA where it received the same review as the Davida case. The NSA Patent Attorney provided the application to the S and P organizations for advice. S recommended that the application not be placed in secrecy and P recommended that it should be placed in secrecy.

This dichotomey prevailed between the S and P organizations when they reviewed cryptographic patent applications because of the perspective from which the applications were judged.

[redacted] The conclusion, that represented the organizational view, was generally arrived at by the judgement of a very few people, sometimes no more than two or three amongst the S and P organizations. The review was not a very structured process and normally involved the same personalities resident in the organization. In any case, the advocate of classifying the application generally prevailed. (b)(3)-P.L. 86-36

The Patent Office was advised that if the Nicolai invention were implemented on a broad basis throughout the world, [redacted] This advice prompted the Commissioner of Patents to issue a secrecy order on 21 April 1978. Nicolai reacted to the news by hiring a Washington, D.C. public relaions agent named Peter Olwell. He immediately corresponded with the Director, NSA and Senator Magnuson of Washington State seeking reconsideration of the Agency's decision. Olwell was advised by NSA General Counsel, Daniel B. Silver, that the Agency would reexamine its recommendation. Nicolai also retained the legal services of Fendler, Fendler, Fendler and Fendler of Beverly Hills, California.

Silver advised DDO, DDC and DDR that the Nicolai invention presented some of the same issues that came to light in the University of Wisconsin patent application. Silver had previously staffed the draft NSA regulation 80-1, a formalized procedure within NSA to examine patent applications, with the various Deputy Directorates and wished to implement the procedure in the Nicolai case, although the regulation was not as yet adopted. Silver felt that it was time for NSA to document its' actions as prescribed in the draft regulation. He instructed that the findings of the Deputy Directorate representatives should be written. If the

recommendation was to continue the secrecy order then supporting reasons must be detailed. All personnel who reviewed the patent application were required to sign an access acknowledgement.

The review group examined the specifications submitted with the patent application and felt that it would be more advatangeous to examine a prototype copy of the device from Nicolai. As compensation, NSA offered a $ 2,000.00 rental fee and told Nicolai that this would greatly expedite the re-evaluation process of his invention. Nicolai's attorneys informed Silver that their cilente was not interested in a rental arrangement but would sell the device to NSA for no less than $50,000.00. Nicolai believed that NSA was infringing upon his rights as an inventor and he threantened to sue the Agency for 2.5 million dollars if they prohibited him from marketing his invention. During July and August of 1978, all discussions and contact with NSA ceased. The Agency was advised that other remedies would be pursued. Consequently, NSA discontinued further studies of the application of the invention.

Then, on 10 August 1978, Nicolai's attorneys reopened discussions with NSA. They requested that the re-examination be completed. NSA again mustered its forces led by William Lutwiniak, Chief P1. However, before Lutwiniak and company could proceed with the re-examination, additional storm clouds were assembling in the Nicolai camp.

(b)(3)-P.L. 86-36

Again, NSA requested a loan of the device for purposes of testing. The $2,000.00 rental payment remained an offer. The offer was declined by Nicolai and his co-inventors. NSA reacted with an attempt to [redacted] and hopefully obtain valid results that would either reinforce the intial secrecy order or recind it. At about the same time, the situation assumed a character of melodrama.

The first melodramatic manifestation was exhibited at Seattle, Washington television station KOMO-TV. They aired a live demonstration of the crypto device and followed up with a report of the ongoing patent dispute between Nicolai and the National Security Agency. The airing was quickly followed by NBC TV affiliates in Seattle calling NSA and asking about the Nicolai matter. Then Time magazine published an article about the subject. This so concerned Inman that he requested an appraisal of the accuracy of the article. NSA General Councel responded with a memorandum[1] that explained the inaccuracies. The storm clouds however did not subside but only changed direction.

The now public controversy reached the offices of Washington U.S. Senator Warren G. Magnuson, who quickly made

---

[1]Memorandum to Director from General Counsel, Subject: TIME Article on the Nicolai Patent Application dated 28 September 1978.

inquiries of DIRNSA. Inman responded to the Senator with a letter explaining the Nicolai dispute. He pointed out, in particular, that,

> "Mr. Nicolai and his co-inventors did not wish to engage in any further discussions with NSA but rather wished to pursue other courses of action."

Also, Inman told Magnuson of the NSA correspondence with Nicolai's attorney which informed him that NSA was ready to reopen discussions with Nicolai whenever he wished.

While Inman's letter was enroute to Magnuson, the NSA General Counsel's office was logging the receipt of correspondence from a new law firm representing Nicolai. It was a Freedom of Information Act (FOIA) request seeking all materials relating to the Nicolai and Davida patent appplications as well as three other secure communications systems that were patented.

While all of this "pursuit of other courses of action" was unfolding, the Lutwiniak investigative team arrived at the conclusion that the Nicolai, et al invention "need not be continued in secrecy". NSA recommended to the Armed Services Patent Advisory Board that the Nicolai petition for recission be granted."

NSA believed that this ended the matter! It was a problem that began in October 1977 and did not conclude, or so NSA thought, until October 1978. During that year, Nicolai and his co-inventors appeared to be represented by four law firms, a Washington public relations representative and were directly conducting various negotiations, on their own, with various Government officials. All of this activity contributed to a state of confusion and resulted in a number of inaccurate stories that were reported in the press and television. It made it very difficult for NSA to conduct business in a coherent and logical fashion. The situation was pointed out to Aldo J. Test, Attorney at Law, and a represenatative for Nicolai with the suggestion that he act as the focal point in the negotiations for his clients with NSA. Unfortunately, the advice fell on deaf ears and the whole Nicolai situation was a constant barrage of NSA dealing with different organizations and individuals all claiming appointed representation of Nicolai and his co-inventors.

"NSA letter Serial: N0894, dated 25 July 1978 to Honorable Warren G. Magnuson, United States Senate from Director NSA/Chief, CSS B. R. Inman.

"Letter to the Armed Services Patent Advisory Board from NSA General Counsel, Daniel B. Silver dated 6 October 1978, Serial: GC/376/78.

Then, on 11 June 1979, two events occurred that reverberated through the halls of NSA. First, Nicolai was issued the "Notice of Allowance" from the U. S. Patent Office. All that remained was to pay a patent fee and U. S. Patent No. 4,188,580 was issued. Second, Inman received a letter from Nicolai and co-inventor. William M. Raike, telling him how they were gratified by the recommendation of NSA, last October, to have the Secrecy Order imposed on their patent application recinded. They then cited Title 35 USC (United States Code), Section 183, and claimed a minimum two and one-half million dollars ($2,500,000) compensation for damages caused by NSA. They theorized that this was the economic harm they endured as a result of the Secrecy order.

NSA attorneys were tasked to examine the Nicolai claim. They concluded that Nicolai would encounter many hurdles in his attempt to acheive a successful claim. The facts failed to support a finding of negligence or wrongfulness on the part of any Government employees involved. General Counsel consulted with the Department of Justice Patent Attorneys who decided not to deny the claim on its face. Instead, correspondence was sent to Nicoali that requested additional information as to why he considered himself and his colleagues eligible to file an administrative claim. No reply was ever received at NSA or the Department of Justice.

Then other curious events took place in the Nicolai saga. On 22 October 1979, one of Nicolai's attorneys, Robert Fendler of Phoenix, Arizona withrew the FOIA request for information previously requested, without explanation. On 16 January 1980, another attorney named, Jim Walsh of Bellingham, Washington, sent a letter of inguiry to the Army Patent Division asking if the claim sent to DIRNSA on 11 June 1979 should have been filed with the Army. Walsh never explicitly stated that he represented Nicolai. The Army Patent Divison responded to Walsh with a statement that denied the claim. In April, Walsh questioned the Army's denial to which the Army responded that it was based on the grounds that the Nicolai patent had never been withheld. The Nicloai case is the best example of a catalyst that thrust NSA out of the world of cryptographic secrecy and anonimity and into a national public debate over cryptography and particularlly its use in computer security. NSA was to be changed forever; for it now was thrust into public debate as to its role and mission as the premier cryptologic entity of the United States.

CHAPTER 9

NSA EMBARKS ON PUBLIC DISCOURSE

In the case of NSA, the proverb "the cat is out of the bag" would more accurately reflect the situation by re-phrasing the saying thusly, "the cryptologic cat is out of the bag"! The escape of the "cat" occured in September 1978 when NSA Director, Vice Admiral Bobby R. Inman agreed to the first press interview by any Director of the National Security Agency. Inman was well aware that by this interview he had broken with NSA policy of the previous twenty-five years that adhered to public silence.

The interview with Deborah Shapley, journalist for SCIENCE magazine was published in the October 1978 issue. Inman disclosed that he had asked for a dialogue with the academic community over the implications of new research in cryptography and communications security. Inman's words reflected his concern:

> "There's a real question now...given the burgeoning interest in this field, how to protect valid national security interests. One motive I have in this first public interview is to find a way into some thoughtful discussion of what can be done between the two extremes of 'that's classified' and 'that's academic freedom'."

He commented on the two cases of patent dispute involving Davida and Nicolai. In the case of Davida's cipher device, Inman said,

> "the issuance of the secrecy order was a bureaucratic error, because, as it turned out, the material had already appeared in the open literature and so could not be classified. Under procedures then in effect, patent applications that are referred by the Commerce Department to NSA were decided at the middle management level. We did not have any internal system to challenge a decision to classify."

He was concerned about the publicity surrounding the Davida case and that promted his decision to change the patent review process at NSA. He declared that any middle management decision to request a secrecy order on a patent application would be automatically reviewed by a senior level group with the final authority vested in DIRNSA or the Deputy Director. The new review

process applied in the case of Nicolai.

The Nicolai case involved a device to scramble radio conversations and Inman told SCIENCE he personally had authorized the secrecy order. The application was reviewed under the new procedure and there was disagreement among the reviewing principals as to whether it merited classification or not. Inman elected to ask for the secrecy order to be applied. He felt where there was uncertainity, one should err on the side of national security. He compared the public disclosure of cryptographic techniques to the disclosure of Atomic Energy secrets.

He believed that NSA should have authority in cryptographic matters similar to the authority granted the Atomic Energy Commission (AEC). Under the law, the AEC can classify the work of any American that it believes will jeopardize atomic energy secrets. Such clear authority does not exist in the case of cryptography. In fact, DOD attorneys have indicated that such AEC authority, clearly, may not extend to any non-nuclear work with military applications.

Although Inman genuinely sought a solution to the problem, his actions fostered a public notion that private ideas in cryptography were "born classified." This is best illustrated by the following events:

In September 1978, the National Science Foundation (NSF) Director, Richard C. Atkinson suggested to Inman that NSA sponsor unclassified research projects at some universities. This would help prevent future problems, opined Atkinson. If the NSF were to continue on its' natural course, what would NSA do if NSF supported research began to impinge on sensitive areas? It would also have the effect of reducing the NSF support in that corresponding area. Furthermore, the White House was concerned with the decline in recent years of basic research support by Federal agencies. NSA could help reverse that trend.

Inman viewed the Atkinson proposal as "most attractive". However, he felt that some homework needed to be done at NSA and perhaps with other agencies involved in public sector cryptography. Two and half years passed and now NSA was ready to fund the academic research in cryptographic related efforts. In the intervening two plus years, dialogue continued between NSF and NSA. A new Acting Director, Donald Langenberg, was appointed at NSF, but Inman continued as the NSA Director.

Attempts at news media interviews with Langenberg met with his refusal to relate any substance about the NSF realationship with NSA. On the other hand, Inman was quite willing to be interviewed. He was queried about the activities of Leonard Adleman of the Massachusetts Institute of Technology (MIT) and his recent conversations with the NSF. Adleman was advised that parts of his grant proposal would not be funded. It had nothing to do with the

merit of his proposal but was concerned with an "interagency matter."

Inman revealed that the NSF partial denial was based on the reason that NSA wanted to fund the research. In fact, the Adleman proposal was one of two that NSA desired to fund. The other was from Ronald Rivest of MIT, who was Aldeman's colleague.

After the NSF news, Adleman, a theoretical computer scientist, received a telephone call from Inman. He explained that NSA wanted to fund his proposal. Adleman was disturbed, he worried about conditions NSA would exact against his work. What would happen if NSA wanted to classify his work and he refused? And furthermore, his application was with the NSF and not NSA! He viewed the collusion between the agencies as "frightening."

Even Rivest expressed grave concern at the notion of NSA funding such research. He worried about the line between what is and what is not cryptography. He felt it was being pushed in a way that affected their ability to do basic computer science research.

The NSF and NSA funding arrangement was also viewed with skepticism by some members of Congress. Particularly, the House Committee on Government Operations and its' subcommittee on Government Information and Individual Rights. So, in February 1980, the subcommittee invited George Davida and historian - editor David Kahn to join Inman in a panel discussion of NSA's public cryptography policy.

Inman found himself, although expected, confronted by an advasarial group. Kahn argued that "no limitation should be placed on the study of cryptography" and Davida agreed. Inman countered with arguments for support of some regulatory control. Finally, the subcommittee recommended that NSA discontinue the policy of " the less openly published in cryptography", all the better!

The subcommittee disapproved of the relationship between NSA and the NSF. It viewed the recently established NSA funding program as a clear attempt to assume responsibility from the NSF for unclassified cryptographic research. The subcommittee did not disapprove of NSA funding its'own public cryptographic research but made it quite clear that NSA should not interfere with the NSF efforts. They even advocated that NSA be removed from the NSF grant review process.

Inman reacted to the recommendations by directly appealing to others in Congress that he felt were sympathetic to the agency mission. He bypassed his chain of command, Secretary of Defense and the DCI, and went directly to congressman Edward Boland, chairman of the House Intelligence Committee. Inman reasoned that Boland would see that the recommendations of the House Government Operations were contrary to the national interest. Also, Boland's knowledge of NSA activities made him uniquely qualified to review the report. Boland delayed the review request of Inman and time

proved to be an asset. The political situation had changed with the election defeat of Congressman L. Richardson Preyer (D-NC) who chaired the adversarial subcommittee and was the key opponent.

Boland concluded that the issue was not resolved and instructed the Intelligence Committee to take an active part in future discussions concerning public cryptography.

Inman did not restrict his public discourse to the SCIENCE interview. He sought an even wider audience. In January 1979, he gave what he termed an "unprecedent" address to the Armed Forces Communications and Electronics Association (AFCEA). He said the speech was "the inaugural of a new policy of open dialogue with the public."[1]

Traditionally, he noted NSA "has maintained a policy of absolute public reticence" concerning all aspects of its two-fold mission carrying out the signals intelligence activities of the Government and performing its communications security function. He went on to explain:

> Until recently, the Agency enjoyed the luxury of relative obscurity. Generally unknow to the public and largely uncontroversial, it was able to perform its vital function without reason for public scrutiny or public dialogue. NSA's particular field of technical mastery--cryptology--was of little public interest, except for a few hobbyists and historians.
>
> This situation has now begun to change in important ways. One result of these changes is that the Agency's mission no longer can remain entirely in the shadows. Concern for the protection of communications, which for many years was viewed as being of interest solely in reference to government national security information, has now expanded throughout the government and to various important segments of the private sector. In the process there has developed a new and unprecedented nongovernmental interest in cryptology and in communications security. Expanded telecommunications protection activity, both governmental and private, has in turn led to an encounter between the activities of NSA and those of other governmental and private entities and individuals that in many ways is novel...[2]

Inman stressed that he was not saying that all nongovernmental cryptologic activity was undesirable. He believed that the expansion of cryptology in the nongovernmental sector held out the promise of significant advance in cryptology that could be beneficial to the public and private interests. However, he was

---

[1] Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernment Sector", printed in the AFCEA's Journal, March 1979.

[2] Ibid

cautious and lacked a strong view about the use of nongovernment cryptologic products within the United States. He recommended that any restriction on domestic dissemination of such products should be approached "most cautiously and in a highly limited framework." Inman had much less inhibition when it came to the export of technology and equipment, he advocated the strengthening of the regulatory framework. He encouraged restrictions on domestic dissemination where that cryptologic information was likely to have a discernable adverse impact on the national security. The concerns Inman raised were clearly controversial. He urged a full examination of the issues by the Executive Branch, the Congress and interested segements of the public.

Inman's own sense was that much of the apprehension he observed within NSA came from the fact that NSA professionals knew where their own thought processes have gone. The threat was not as much with present day research but more importantly where would the research lead to applications ten years hence. This potential difficulty bore directly upon both the communications security code and cipher systems and the conduct of signals intelligence activities. Inman believed that over the following decade there would be quantum jumps in academia and industry that would catch up to what NSA had already done. Given these various concerns, NSA's public position, in 1980, could be summed up this way.

A great deal of historical information about the nations cryptologic activities must remain under the archivist's lock and key. Public cryptology so far had not broken new ground. Giant strides in the academic and industrial communities over the next decade could erase the Government's classified lead in cryptographic applications. Finally, a line must be drawn somewhere between Government needs and those of basic research. To this end, NSA established a forum with the academic community to determine where and how the line might be drawn.

In May 1979, the Inman call for a dialogue with the Academic Community led the American Council on Education to convene a meeting that recommended establishment of a Public Cryptography Study Group. The National Science Foundation agreed to fund it and the group held its first meeting on March 31, 1980 in Washington, D.C.

All members were present, including Daniel C. Schwartz, NSA General Counsel, Professor Davida, representing the Computer Society of the Institute of Electrical and Electronics Engineers, Ira Michael Heyman, Chancellor-Elect of the University of California at Berkeley, Jonathan Knight, Associate Secretary of the American Association of University Professors and representatives of the IEEE, Association of Computing Machinery, American Mathematical Society and the Society for Industrial and Applied Mathematics. The chairman was Werner A. Baum, Dean, College of Arts and Sciences, The Florida State University, who had been chancellor of the University of Wisconsin's Milwaukee campus when Davida received his secrecy order.

The members of the intial gathering were concerned with how the group should proceed. Baum particularly noted that the NSF, as a condition of the funding, implied a three step process. First, careful and precise articulation of the problems. Secondly, prepared statements of positions on the issues. And thirdly, recommendations on how differences might be reconciled must be submitted to the Director of NSA and the President of ACE by the end of 1980.

As with many groups, the deliberations went beyond the deadline and discussions ensued to the last meeting held in February 1981. The results were not what NSA had expected. Inman proposed a set of restrictions on domestic dissemination of nongovernmental technical information related to cryptology. Further, he proposed a prepublication review wherein it would be a crime to publish without seeking permission. The membership concluded that the proposal was a clear violation of the First Amendment protections to "commercial " speech that was ruled by the then sitting judges of the Supreme Court.

The committee, although sympathetic to Inman's concerns, suggested that a voluntary system be established. It would follow the constraints voiced by Inman, however there would be a clear understanding that submission to the process was voluntary. Neither the authors nor the publishers would be required to comply with the suggestions or restrictions urged by NSA.

One of the members of the group, George I. Davida voiced strong objections to the voluntary system. In fact, he felt so strongly about his views, Davida authored a separate paper as "A Minority Report of the Public Cryptography Study Group of the American Council on Education". He argued against any restraints on nongovernmental cryptographic research.

He reasoned that any restraints would adversely affect the quality and direction of basic research in computer science, engineering and mathematics. Besides, the likelihood of basic research producing cryptanalytic attacks against NSA cryptosystems he believed to be nil. The restraints, even if they were desirable and possible, would be ineffective.

Cryptography is largely an intellectual process in which the design and analysis of algorithms could be implemented on any abudantly avaiable microprocessor. The design of cryptosystems involves a large degree of distrust and suspicion about the possibilty that the system will have a short cut known only to the designer. Thus, as David Kahn had pointed out, governments are unlikely to trust anyone but their own scientist and engineers. Certainly, governments would view the design of U.S. cryptosystems as an opportunity for the U.S. to conduct intelligence gathering.

Although the Study Group was just that, a study group chartered to make recommendations, Davida feared their recommendations. He was concerned that if NSA was not satisfied

with the outcome of the voluntary system it would seek legislation. And the legislative hearings could conclude that the group recommendations were expert testimony that would validate the NSA claims. He labelled any such conclusion as completely erroneous. After all, the majority of the committee members were not engaged in research in data security or cryptography. Davida summarized his opinions thusly,

> "... I find NSA's effort to control cryptography to be unnecessary, divisive, wasteful and chilling. The NSA can perform its mission the old fashioned way: STAY AHEAD OF OTHERS."[11]

NSA accepted the voluntary system in May 1981 although the Operations Directorate viewed the whole process as a withdrawal from the goals of strengthening dissemination restrictions. The voluntary system received wide publication in the professional journals. Participation was modest, but it is interesting to note that Davida submitted papers for review.

Inman was to confront other issues involving communications security. Those issues had there roots in the non-defense side of the U. S. Government. In addition to the National Bureau of Standards and the adventures of DES, the Ford administration had conducted discussions about ways to secure public and private telephone messages in the United States. Their concern was about the possibility of intercept from microwave towers and satellite communications by the Soviet Union and other foreign countries. His administration sought the advice of the Director of the Office of Telecommunications Policy (OTP).

The Presidents' National Security Council, in the fall of 1976, requested the OTP to draft a plan that would address these concerns. A plan was drafted by December of 1976, but it had to await the judgement of a newly elected President Carter. The OTP plan evolved into the Presidential Directive/NSC-24, commonly referred to as PD-24. Signed by President Carter on 16 November 1977, it called for improved telecommunications protections for government derived, unclassiifed information which may be of value to a foreign adversary.

The directive was significant from two perspectives. First, it officially acknowledged that some unclassified information required protection. Second, it assigned that protection responsibility of some U.S. government communications to an agency outside of Defense. That agency was the Commerce Department. Why the Commerce Department and not NSA?

---

[11] A Minority Report of the Public Cryptography Study Group of the American Council on Education entitled, "The Case Against Restraints On Non-Governmental Research in Cryptography by George I. Davida, February 1981.

The answer was found in the views of the National Security Council Staff. They were determined to maintain the lines of mission responsibility and the charter of NSA permitted only foreign intelligence collection. Never, under any circumstances, would it be appropriate for an intelligence agency to monitor or have access to the communications of Americans. The policy was reinforced in light of the Watergate debacle. In effect, the directive now divided the responsibilities of communications security between NSA and the Department of Commerce. Commerce was faced with the problem of devising new protection measures that would be independent of NSA and its products.

The Secretary of Commerce selected the National Telecommunications and Information Administration (NTIA) to execute the responsibilities assigned to the DOC by PD-24. The NTIA was formed at Commerce through the disestablishment of two offices, the Office of Telecommunications within DOC and the Office of Telecommunications Policy of the Executive Office of the President.

The NTIA established a Special Project Office. But, why was NBS not involved? Afterall, they were the focal point for DES at Commerce! Well, the old hands from the former offices comprised the membership of the new NTIA and they viewed the implementation of PD-24 as the execution of policy issues and not primarily a cryptographic concern.

The policy would stress the need to preserve a climate of freedom with minimal government interference in the private sector. It also fostered the elimination of restrictions expressed in the International Traffic in Arms Regulations (ITAR) and secrecy patents. The ITAR auxiliary military equipment category specifies speech scramblers, private devices and cryptographic devices for encoding and decoding.

This view was a direct confrontation of NSA's admonitions that extensive public work in cryptography and related fields would have a significant potential adverse impact on national security.

The conflict between Commerce and DOD (mainly NSA) was made known to Dr. Frank Press, the Director of the Office Of Science and Technology Policy with the intent of having the issues resolved. But, the recent Presidential election results changed the political landscape. Ronald Reagan was now President of the United Srtates.

Congressman Boland, Chairman of the House Intelligence Committee, supported the NSA position on public cryptography. He informed President Reagan:

> (The NTIA proposal) leads me to have serious reservations about the advisability of PD-24's dichotomy of responsibility. The NTIA analysis does not examine national security concerns in reaching its conclusions. Rather, it attempts to define away such concerns in its

promotion of a public cryptography policy which will export all but 'very high-quality encryption technology'... It further states that 'effective control of the export of technical data on cryptography is not feasible.'

Such observations not only reveal an ignorance of U.S. cryptology problems, they ignore the fundamental purpose of PD-24, the protection of U.S. cryptology secrets...

There seems little doubt that non-government use of cryptography will expand greatly in the next decade. The legitimate concern of the U.S. Government ought to be to insure that this expansion does not conflict with the protection of national security concerns...

PD-24 should be reexamined. I urge you to institute such a review in order to restructure this essential element of national policy..."

A review of PD-24 resulted in it being replaced on September 17, 1984 by National Security Decision Directive Number 145, signed by President Ronald Reagan. It established the Director, National Security Agency as the National Manager for Telecommunications and Automated Information Systems Security. It established NSA as the government focal point for cryptography, telecommunications systems security and automated information systems security. This Directive was the root document responsible for the establishment of the National Computer Security Center at NSA. It gave NSA a new mission in addition to its' classical missions of SIGINT and COMSEC. NSA was now charged with the responsibilities of national management of the security of automated information systems better known as COMPUSEC (computer security). The evoultion of NSA as National Manager is a history that is directly involved with the history of the National Computer Security Center. A story yet to be written!

---

[1]Congressman Edward Boland, Letter to President Ronald Reagan, 3 February 1981. (U)

APPENDIX B

REVISED COMSEC FUNCTIONS OF NSA

1. Create, prescribe or approve the cryptoprinciples incorporaterd or to be incorporated in any COMSEC equipment, telecommunications system, weapons system or space vehicle system used by the departments and agencies of the Government. Included in this are all forms of encryption techniques, whether embodied in separate equipment or incorporated into a computer program and whteher such techniques are intended to prevent or delay recovery of intelligence from transmitted signal or for the purpose of impending detection, interception or jamming of transmissions.

2. Devise and prescribe, or review and approve, rules, regulations and instructions governing the application, operation and use of any COMSEC equipment or encryption techniques, including those embodied in computer programs, and, as necessary, restraining or removing from use any equipment or encryption technique considered unsuitable or unsafe.

3. Perform technical analysis for the purpose of determining the degree of COMSEC actually being achieved within any secure communications, weapons, or space vehicle system by the combination of encryption equipment or techniques, system configuration, operating procedures (including appropriate computer software) and physical security practices employed throughout the system; included in this is the recommendation to the appropriate department or agency of the level of classification of information which may be safely passed in the specific system.

4. Develop techniques, equipment and doctrine needed to prevent or control compromising emanations of classified information, whether processed within or transmitted by a secure communications, weapons, or space vehicle system.

5. Establish security standards for protection of classified information stored in, processed by, or exchange between, time-shared multi-access computers.

6. Control, within Board policies, the release of crypto information, equipment, keying material, or techniques to foreign nations and to U.S. contractors; included are computer encryption software, compromising emanation information, and low detectability and anti-jamming techniques based on cryptoprinciples.

The above was a draft proposal to a re-write of the National Security Council 5711 directive designating the Director, NSA, as the Executive Agent of the Government for all COMSEC matters. In the re-write a specific reference to computers and there applications was deliberate since the previous NSC 5711 was written before the advent of the computer security issues.

The COMSEC view of computers was viewed somewhat thru "tunnel vision". That view fostered by dealing, in the majority of field cases, with "imbeded" computers. That is, the systems requiring COMSEC applications were systems not associated with constant and programmable human manipulation.

Computers played a major role in providing the communication field with tools to meet the new requirements of handling larger volumes of information at faster speeds. The COMSEC organization had been involved in three communication areas which employed computers; record switching, voice switching and computer compartmentation. The reason for the COMSEC involvement in each area was because the computer played a significant role in providing part of the overall security to these communication activities.

The record switching computer performed the function of receiving incoming messages or data from terminals, storing the messages or data for a relatively short period of time and then forwarding the message on to the addresses of the message or data. When using computers for record switching of classified information COMSEC must be considered. In order to establish security guidelines for computers, NSA published the "Security Standard for Sophisticated Record Communications Switching Centers." The purpose of the standards was to insure the optimum security of the transmitted information and maintain the security within the switching center comparable to that provided during transmission of the message. The standards covered three major areas; compromising emanations, misrouting of messages (when a message of a certain classification is sent over a line or to a terminal that is of a lower classification) and intelligent deception.

In October 1965 NSA published "COMSEC Standards for Secure Voice Communications Systems" and this standard applied to all secure voice communication systems. The purpose of the standard was to establish criteria to insure optimum overall security of voice communications.

The 1967 definition of computer compartmentation was defined thusly, "computer compartmentation is when there are various levels of security cleared terminals that have direct access to process or handle classified information in a common computer." The idea of using computers on a time sharing basis was a new concept in 1967, made possible by the introduction of advanced computers commonly referred to as third generation machines. The introduction of the machines prompted many federal agencies to allow terminals of different security level authority to access a time shared computer containing various security levels of information. These actions fostered the growth and impetus for computer security. Committees were formed to develop standards for computers that handle multilevel security information at the terminal. Such activity was witnessed by the COMSEC organization in places like Advanced Research Project Agency (ARPA), the WWMCCS network and in companies like the System Development Corporation.

APPENDIX C

NSA Roles and Responsibilities in the Field of Computer Security

1. The purpose of this policy is to establish the NSA roles and responsibilities in the field of computer security and to present basic guidance as to how they will be fulfilled.

2. COMSEC - By National Security Council Directive, dated 26 August 1968, the Director, NSA, is responsible for designing, developing, evaluating, producing and authorizing for use all cryptographic systems and command authentication systems employed by the United Staes Government.

3. SIGINT - Under DCID No. 6/3, and as a member of USIB, the Director, NSA, is responsible for establishing standards for the protection of COMINT transmitted electrically, as well as for insuring that COMINT under his physical and/or operational control, is protected in accordance with DCID No. 6/3 requirements. Under Annex E to DCID NO. 6/3, the Director, NSA, is also responsible for proposing to the USIB "policies and procedures for erasing, or othrewise securing used magnetic storage devices (employed in the ADP processing of COMINT) and for their classification, reuse, storage, and shipment."

4. EMSEC (Emanations Security) - Under its charter responsibilities, the USCSB is charged with the development and promulgation of national policy and technical guidance on EMSEC. As a member of that Board, the Director shares responsibility for developing and approving such policies and guidance. As the head of a Government agency which develops and/or uses information-processing (including ADP) equipment subject to radiation vulnerabilities, he is responsible for incorporating appropriate suppression or other radiation countermeasures into such equipment or facilities under his cognizance, in accordance with the promulgated guidance.

5. Physical and Personnel Security - As the head of a National agency which handles classification defense information, The Director, NSA, is responsible for compliance with Public Laws, Executive Orders, DCID NO. 6/3, and implementing Department of Defense Directives governing the physical protection of and personnel clearance requirements for access to such information. He is additionally responsible for establishing and implementing any additional "need-to-know" controls deemed necessary for the protection of classified information processed, produced or used under NSA jurisdiction or cognizance.

6. Development/Use of Computer Systems - For those sysytems which he develops, the Director, NSA, is responsible for providing protective features commensurate with the threat of classified information loss. Where the threat is possible exploitation by hostile parties and/or uncleared users, COMSEC

measures are called for; where the threat is possible loss of information to a cleared user of the system whose clearance is not at the appropriate level or who has no "need to know", other security measures will normally be sufficient. As a user, the Director, NSA, is responsible for implementing appropriate physical and personnel security controls at those facilities under his cognizance and for implementing the COMSEC, EMSEC and Prescriptive/Restrictive Control measures which the application and usage conditions of the system indicate are required. Other developers and users have identical responsibilities.

7. Technology Leadership - NSA has long recognized a moral responsibility to provide leadership and assistance in fields in which it has particular expertise, even though it does not have, nor does it seek, formal responsibility. Of particular importance is NSA's preeminence in the field of computer technology as applied to intelligence operations. Because of this fact, this Agency has a special obligation to provide leadership and assistance on computer security problems to member activities of the intelligence community where the protection of information is a shared responsibility. Beyond that community, however, NSA will aggressively pursue only its COMSEC role and assume responsibility for providing assistance only where a COMSEC requirement is clearly indicated. In all other cases, NSA assistance, when requested, will be confined to the provision of general advice or conceptual information on typical Prescriptive/Restrictive Control techniques which have been developed, used and validated as being adequate by this Agency. NSA will not assume responsibility for evaluating or approving specific Prescriptive/Restrictive Control measures, supervisory routines, other protective software programs or system operating procedures developed or being considered by others for use in computer systems in which we have no direct operational involvement. To do so would be to render a disservice to the requesting authority, because as a pratical matter such evaluation or approval (formal or tacit) would, in the typical case, be based on incomplete information and therefore might be invalid. Futhermore, it may be completely invalidated by subsequent hardware or software changes. This responsibility properly rests with an authority who is in direct control of the system's operation and who is in a position to maintain detailed and current knowledge of all program changes.

8. For the purpose of this policy, the following definitions pertain:

a. Computer security is the protection resulting from all measures designed to prevent either deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification or loss of information contained in the computer system and introduction of information into the system.

b. Information includes both classified data, and computer programs for control of classified data and systems operation.

c. COMSEC encompasses certain aspects of computer security when the computer is part of a secure federal telecommunications system. It includes that protection against exploitation via telecommunications. It does not include the protection resulting from the physical security measures designed to protect the controlled area housing the computer, or other physical security measures except those needed to protect COMSEC equipment, components and material.

d. Secure federal telecommunications refer to U.S. Government associated systems and may include those systems which the U.S. Government shares with allied governments.

e. A computer is considered part of a telecommunications system whenever there is a direct communications link from the computer which extends beyond the controlled access area housing the computer.

NOTE: This definition is intended to cover any computer system (including time-shared and/or multi-level access) which has remote terminals, as well as a computer used for switching in a communications system.

9. There are four distinct applications of computers which involve security considerations of varying degrees of importance and complexity. The first, and simplest, case is a dedicated, self-contained computer complex which is used to process classified information; the entire facility is under the operational and physical control of its user, he is the only user, and he is soley responsible for insuring that the data it processes is adequately protected. The second type of application is one involving alternate use of common equipment where classification of the data and the authorized access level of users may range from unclassified to the most sensitive classified level. The unique problem in this circumstance is the provision of means to insure that the computer is cleared of data which the next user is not authorized to know before the facility is made available to him. The third type of computer utilization is one in which the computer is employed as an integral part of a secured communications or command and control system to perform cryptographic, switching or related traffic handling functions; NSA's responsibilities with regard to this type of computer application are clearly defined in its COMSEC charter and are appropriately assigned internally. The fourth type of computer usage is one in which remotely located computers exchange data over interconnecting communications links or in which a single computer or computer complex serves a number of individual subscribers on a time-shared basis, each of whom has access to remote terminal from which he can control the computer to obtain information from it. This fourth type of application is the one that is primarily addressed herein.

10. Requirements for the protection of data processed by time-shared, multi-access computers fall into four categories. These categories are not mutually exclusive; in a given computer

terminals are authorized to process.

(2) Prescriptive/Restrictive Control measures, including operating procedures and routines incorporated into the computer logic and associated supervisory programs or other software which are designed to prevent the computer from executing unauthorized input/output orders or instructions. COMSEC measures are not necessarily required for this purpose.

(3) Storage media control procedures.

(4) Continual monitoring and surveillance of the system's operation to assure prescribed security measures are operable and to identify attempts to circumvent them.

d. For Category 4 (to segregate officially unclassified information among users of the system):

Control measures, similar to those specified for Category 3, are adequate. No COMSEC measures will normally be made available for these unclassified applications.

12. Procedures and Responsibilities:

a. ADC and ADRD, in their respective functional areas, are responsibile for establishing COMSEC standards and for developing and providing the COMSEC measures to satisfy Category 1 and 2 requirements of all Federal departments and agencies.

b. ADP is responsible for providing or approving and maintaining cognizance over the Prescriptive/Restrictive Control measures (computer logic, software routines, installation, operating and surveillance procedures and protection of storage media) for computer systems developed and/or used by NSA independently or in conjunction with other members of the SIGINT community.

c. Chief, Office of Security, is responsible for prescribing and maintaining cognizance over physical and personnel security measures to satisfy Category 1, 2 and 3 requirements at all computer facilities and terminals under NSA jurisdiction or cognizance. M5 will also provide advice and guidance in the development of methods and procedures for counterintelligence monitoring or surveillance over system operations.

d. ADRD is responsible for conducting a continuing program of research into technological "computer security" vulnerabilities from the standpoint of both hardware and software considerations, and for developing effective protection methods for countering such threats.

e. Commandant, National Cryptologic School, is responsible for coordinating or providing support for "computer security" training requests.

f. ADN is responsible for:

(1) Promulgation of coordinated NSA policies and procedures in computer security.

(2) Assuring that responses to outside requests for assistance on computer security problems are coordinated and consistent with the policies in paragraph 7 above.

(3) Coordination of internally or externally proposed policy changes or additions to National or DOD Directives in the computer security field.

g. ADST is responsible for maintaining overall cognizance of the various technical activities being pursued by NSA and others in the field of "computer security".

It is important to note that the above policy was for internal use within the confines of the National Security Agency and provided assistance only where a COMSEC requirement was clearly indicated. In all other cases, NSA assistance, when requested, would be confined to the provision of general advice. This policy reflected the general view amongst the major internal NSA organizations. That view was expressed in the words that communications security was our sole responsibility; the denial of access to information stored in a computer or the protection against TEMPEST or other exploitations of computer manipulated data did not automatically come within the Agency baliwick.