3-9-2010

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

FOIA Case: 60251A
27 February 2010

Mr. John L. Young
251 West 89th Street
New York, NY 10024-1739

Dear Mr. Young:

This further responds to your Freedom of Information Act (FOIA) submitted via the Internet on 25 November 2009, which was received by this office on 27 November 2009, for all documents pertaining to a letter written by Joseph A. Meyer to the IEEE in August 1977 concerning possible ITAR violations of cryptography research exported to countries outside the United States unless by export license, including the actual letter. We responded with an initial response on 18 December 2009 and provided you with two documents. We also noted that we could not locate the actual letter written by Joseph A. Meyer.

Enclosed is an additional document containing information you requested. Additional information responsive to your request continues to be processed under the provisions of the FOIA. We will inform you of our release decision regarding that information upon completion of our processing.

Sincerely,

for Sally A. Nicholson

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encl:
a/s

Vice Admiral B. R. Inman, USN

The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector

Editors Note: Published here is the address delivered by the Director in the Friedman Auditorium at the March 1979 meeting of the Computer and Information Science Institute.

I am privileged to have the opportunity to exchange with you this morning some views on what has been happening to NSA in the public sector with regard to growing interest in public cryptography, to give you some background on what is going on in our trying to deal with that problem, and then to throw the forum open for questions.

When I came to the job in July 1977 I found early on that we were subject to constant newspaper articles which implied NSA's involvement in activity in a manner that was uniformly critical of the Agency, and sometimes publishing information that was of broad public interest, the media would unnecessarily include commentary on NSA being the source, with all the immediate damage to sources and methods that would accrue. A lot of dialogue ensued, which involved several senior executives from the Agency. The end result was a conscious program, low-key and carefully paced, to try to get across, by means of private contact, the Agency's concerns. An active commitment was made last August to give a public speech expressing NSA's concerns before the Armed Forces Communications Electronics Association — a group of people with good cause to share our concerns, and, in all honesty, a group that we judged would be a reasonably friendly forum. Much advice and assistance throughout this process came from a good many people in the Agency. I will run through it again for you now much as it was presented to two AFCEA public forums. When I finish, we will be prepared to discuss with you "where does this leave us and where is it going to go." You should know that in the back of my mind, as this process has gone on, is the thought that we will eventually need some additional constraint mechanisms; whether those are legislative or whether they are orchestrated out of agreements with the academic community and the Executive Branch and industry remains to be seen. But part of the effort in doing this whole cautious public dialogue is to try to create a climate which does not stampede to introduce changes inimical to our interests, and which, if we need it, would provide the basis of some public understanding for future legislation. The text goes as follows:

* * * * * * *

This is the second time I have spoken to members of this organization concerning a matter of great concern to the National Security Agency. As you know, a public discussion by an incumbent Director of the National Security Agency on a subject related to the Agency's mission is an event that is at least unusual, if not unprecedented. My talks with this group — today (this was in Los Angeles on 12 February) as well as at the January Symposium in Washington — represent a significant break with NSA tradition and policy. The reasons for this break will be the principal subject of my remarks. The fact that I have chosen this group for the inaugural of a new policy of open dialogue with the public is not fortuitous. It reflects

Approved for Release by NSA on 02-25-2010, FOIA Case # 60251

the high regard I have for this organization and its members and for the contributions you have made to the field of communications.

Traditionally, NSA has maintained a policy of absolute public reticence concerning all aspects of our mission. As you know, that mission is two-fold. First, it consists of carrying out the signals intelligence activities of the United States Government. The second mission of the Agency is to perform the government's communications security function. As currently defined, this means the protection of the security of U. S. Government communications related to national security and those communications of government-related entities (such as government contractors) that contain national security or national security-related information. In both these capacities, the Agency executes the responsibilities of the Secretary of Defense, who has been named by the President as Executive Agent for Signals Intelligence and Communication Security.

From my vantage point of 19 months of close and intense observation, I can assure you that the Agency serves the government and the people of the United States extraordinarily well in the performance of both missions. Some of you probably are familiar with the Agency's communications security mission as a result of your work as contractors or otherwise. NSA's accomplishments in that field are due to a fruitful interaction between the talents of our own employees and those of private industry.

In the signals intelligence field, the Agency has, since its inception in 1952, provided a vast quantity of intelligence information of inestimable value in the conduct of the Nation's defense and foreign policy. NSA's ability to provide such intelligence information has rested — and will continue to rest — on maintaining a high degree of secrecy about all aspects of its intelligence mission. The conduct of that mission is based on intelligence sources and methods of the utmost fragility and sensitivity. Disclosure of information about such sources and methods poses unacceptable risks that they will be irretrievably damaged.

Consequently, the Agency has traditionally engaged in secrecy to an extraordinary extent. Our employees have accepted the sacrifice of not telling their spouses and their families what they do, and frequently the no less significant sacrifice of not knowing much about what goes on elsewhere in the Agency or even in the same office. Until recently, the Agency enjoyed the luxury of relative obscurity. Generally unknown to the public and largely uncontroversial, it was able to perform its vital functions 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 the 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 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 a novel encounter between the activities of NSA and those of other governmental and private entities and individuals. My purpose today is to describe to you some of the new trends, developments and concerns that have led to this encounter and to describe to you, from NSA's perspective, some of the major concerns and policy issues that stem from growing nongovernmental interest in telecommunications protection.

The underlying message I would like to leave with you is that to define a necessary level of telecommunications protection and to achieve that level of protection gives rise to complex tensions between the intelligence and national security interests of the government, on the one hand, and the telecommunications security interests of both the public and private sectors, on the other. These tensions and the resulting policy issues to which they give rise are real. They will not go away if we pretend they do not exist. And I believe that there is a very real risk, in the absence of a prompt and serious effort to confront and resolve them, that damage will be done to the national security. Because in the private sector the industrial and academic worlds are the principal focuses of interest in questions relating to telecommunications protection, I am striving to open up a dialogue between the Agency and these portions of the private sector. The hope is that such a dialogue will lead to a better understanding by all parties and eventually to the development of an approach to the problem in which the legitimate interests of all sides can be protected. I do not expect to leave you today with any firm answers. I do hope to be able to describe to you the nature of the problem and the issues which need to be confronted and earnestly to solicit your views and your help during the coming months and years.

Viewed from NSA's perspective, the crux of the problem is that increased concern over telecommunications protection in the nongovernmental sector im-

plies increased public knowledge and discussion of communications protective techniques. The principle such technique, of course, is cryptography. There is a very real and critical danger that unrestrained public discussion of cryptologic matters will seriously damage the ability of this government to conduct signals intelligence and the ability of this government to protect national security information from hostile exploitation.

I am not saying that all nongovernmental cryptologic activity is undesirable. To the contrary, the expansion of involvement in cryptology in the nongovernmental sector holds out the promise of significantly advancing the state of the cryptographic art in ways beneficial to both public and private interests. What I am saying, however, is that the very real concerns we at NSA have about the impact of nongovernmental cryptologic activity cannot and should not be ignored. They must be given full consideration in the working out of an accommodation between public and private interests. Ultimately these concerns are not merely those of a single government agency, NSA. They are a vital interest to every citizen of the United States, since they bear vitally on our national defense and the successful conduct of our foreign policy.

Today, for perhaps the first time in history, we have in this country a strong and growing nongovernmental interest in telecommunications protection and in privacy. Both of these imply the use of encryption as a major protective technique. In addition, we have a growing interest in cryptology as an academic or scholarly discipline for reasons that seem to be only partly related to the growth of interest in cryptography for protective purposes.

I would like to sketch briefly for you some of the key developments and factors in this situation which have led me to the conclusion that the time has come when a dialogue is necessary on the relation between governmental and nongovernmental activity in telecommunications protection or, more specifically, on nongovernmental cryptologic activity. In passing, I would like to set the record straight as to NSA's involvement in certain somewhat controversial recent developments.

- There is a growing recognition of the potential vulnerability of our communications system within the United States to exploitation, both by foreign powers and by domestic law-breakers. There has been considerable attention paid in the Congress and in the press to the perceived threat of exploitation of domestic communications by foreign powers. As you know, several Administrations have taken this problem very seriously and this Administration has set in motion a program of governmental activity designed to increase the ability of the non-national security portions of the private sector to identify communications vulnerabilities and to take appropriate protective measures.

- There has been a growing public concern over the protection of data generated by or stored in computers. The public has become increasingly aware of the danger that automated data processing systems, if not adequately protected, can be exploited for fraudulent or illegal purposes. Moreover, the vast amounts of personal information stored in and handled by automated data systems, both private and governmental, has given rise to serious concerns about individual privacy. In the governmental sector, these concerns find expression, in part, in the 1974 Privacy Act which many read as imposing an obligation on the government to protect the security of personal information stored in government automatic data systems.

- Impelled by the factors I have just described and acting under the authority of the 1965 Brooks Act, the National Bureau of Standards undertook to develop a data encryption standard (usually referred to as DES) to serve as the standard for protection, by encryption, of information in computers purchased or used by the Federal Government. The development of the DES is an area in which NSA has interacted with the non-national security segments of both governmental and private sectors. This interaction has been the subject of untrue and irresponsible allegations to which I will return shortly.

- The existing statutory and regulatory framework for controlling the dissemination of potentially harmful cryptologic information has become embroiled in a certain degree of public controversy. Many of you no doubt are familiary with the concerns expressed by elements in the academic community that the International Traffic in Arms Regulation (commonly called the ITAR) may serve to inhibit international exchanges of basic scientific information. I will also return to NSA's role in this matter in a moment.

- In two recent incidents, the Commissioner of Patents and Trademarks has, on NSA's advice, imposed secrecy orders under the Invention Secrecy Act on cryptologic inventions submitted for patent. In both cases, these orders were subsequently withdrawn, but both incidents gave rise to substantial discussion in the press and a good deal of comment unfavorable to NSA.

- To cite another development, there has been a spate of recent scholarly activity in the cryptologic field. This has included publication of books and articles setting forth sophisticated attacks on commercially available cryptographic equipment, as well

as the conduct of international seminars on cryptographic matters by noted U.S. experts.

• Finally, there are indications that companies are becoming interested in non-national security telecommunications protection as a promising new commercial market. While I have no basis for quantifying the size of such a market, I am aware that many forecast a substantial growth, both domestically and in terms of exports, in demand for crytographic and other communications protection devices for non-national security applications.

All of these factors, and others, bring me to the conclusion that it is time for NSA's concerns and NSA's own role in this complex field to be better understood. To the extent NSA has been involved in the developments I have just listed, the Agency's role has been widely misrepresented. Insofar as I can within the severe constraints imposed by the secrecy necessarily associated with many of our activities, I would like to clarify the concerns I feel must be accommodated in the future development of nongovernmental telecommunications protection activities.

First, let me set the record straight on some recent history. NSA has been accused of intervening in the development of the DES and of tampering with the standard so as to weaken it cryptographically. This allegation is totally false. It should suffice to point out that the Senate Select Committee on Intelligence made an exhaustive investigation of these allegations. Their conclusion was a categoric rejection. Quoting from the unclassified staff report of the Committee: "NSA did not tamper with the design of the algorithm in any way. IBM invented and designed the algorithm, made all pertinent decisions regarding it, and concurred that the agreed upon key size was more than adequate for all commercial applications for which the DES was intended." The implausibility of public allegations is further demonstrated by the fact that NSA has endorsed the use of DES for the encryption of national security-related information, including selected classified information.

Another allegation is that the Agency has attempted to suppress scholarly work in cryptology through the use of the ITAR and the Inventions Secrecy Act and by exerting pressure on the National Science Foundation. These allegations are baseless. The charge relating to the ITAR arose, in large part, from an unfortunate incident in which an NSA employee, a member of the Institute of Electrical and Electronics Engineers, wrote a letter in his private capacity to the IEEE, suggesting that certain symposia and the publication of papers on cryptology might be in violation of the ITAR. This incident, too, was investigated by the Senate Select Committee on Intelligence, which found that the letter in question was entirely a personal initiative, had not been sponsored by the Agency and did not represent any attempt by the Agency to inhibit scholarly activity. And here on each occasion I have inserted into the text the parenthetical comment that there were a great many who believed that the individual in his private capacity was also correct in his evaluation.

The agency has also recognized that ambiguities in the definition provisions of the ITAR could be viewed as inhibiting international scholarly exchanges on matters relating to cryptology. Another ambiguity in the regulation could be viewed as imposing a requirement of prior governmental review on domestic scholarly publication. The Agency has taken the lead within the Executive Branch to attempt to clarify the ITAR so as to allay any fears that it may improperly apply to scholarly activity. As a result of NSA initiatives, I understand that the Office of Munitions Control is reviewing the matter and, if appropriate, will issue a clarifying statement that will meet the concerns expressed by the scholarly community.

In the Inventions Secrecy area, there has existed for many years a statutory provision permitting the Commissioner of Patents and Trademarks to impose a secrecy order on any invention submitted for patent, the public disclosure of which could be detrimental to the national security. In two recent cases, NSA imposed secrecy orders, which intensive and continuing technical review by the Agency later permitted to be withdrawn. NSA's actions were attacked as an attempt to prevent the American public from enjoying telecommunications protection so as to permit NSA to intercept domestic communications. Nothing could be further from the truth. NSA has no interest in and indeed is legally precluded from intercepting domestic communications not involving foreign powers. Deliberate interception of the communications of United States persons in the United States now requires court approval under tightly drawn criteria. Extensive legal restrictions have been embodied in the recently passed Foreign Intelligence Surveillance Act of 1978. In sponsoring secrecy orders under the Inventions Secrecy Act, the Agency's sole consideration is the detrimental effect on the Agency's mission, and thus on the security of the United States, that would result from the proliferation abroad of sophisticated cryptologic technology.

Equally baseless is the charge that NSA exerts some kind of undue influence on the National Science Foundation research grant decisions. While NSA does play a peer review role with respect to such applica-

tions in the field of cryptology, that role has been limited to commenting on the technical merits of proposals.

These allegations (and others that have appeared from time to time in the media) paint a false picture of NSA as exerting some kind of all-powerful secret influence over all the government from behind closed doors. I can assure you from 19 months experience that this is far from reality. The truth is that the legal resources of the Federal Government to control potentially harmful nongovernmental cryptologic activity are sparse. Under the ITAR, the government can prevent the export of harmful cryptographic equipment and some foreign dissemination of technical information having a direct relation to cryptographic equipment. There are, however, to my knowledge, no limitations whatsoever on publication of such nongovernmental information within the United States or on the export of such publications. The Inventions Secrecy Act provides a very limited possibility of imposing secrecy on potentially harmful inventions. I say "very limited" because the Act applies only if an application for patent is made and, obviously, is effective only to the extent public disclosure has not already occurred before the secrecy order is issued. In the application of both the ITAR and the Inventions Secrecy Act, NSA plays a technical advisory role but is not the final decision-making authority.

While some people outside NSA express concern that the government has too much power to control nongovernmental cryptologic activities, in candor, my concern is that the government has too little. I believe that there are serious dangers to our broad national interests associated with the uncontrolled dissemination of cryptologic information within the United States. It should be obvious that the National Security Agency would not continue to be in the signals intelligence business if it did not at least occasionally enjoy some cryptanalytic successes. Application of the genius of the American scholarly community to cryptographic and cryptanalytic problems, and widespread dissemination of the resulting discoveries, carries the clear risk that some of NSA's cryptanalytic successes will be duplicated, with a consequent improvement of cryptography by foreign targets. No less significant is the risk that cryptographic principles embodied in the communications security devices developed by NSA will be rendered ineffective by parallel nongovernmental cryptologic activity and publication. All of this poses clear risks to the national security. While I cannot go into further detail without exposing matters that must remain secret, I can tell you that I have not lightly accepted the position that unrestrained nongovernmental cryptologic activity poses a threat to the national security. I have caused senior NSA officials personally to examine every premise and all of the evidence underlying this conclusion and have reviewed their work in a spirit of great skepticism. Nevertheless, after going through the exercise, I have a deep conviction that the national security missions entrusted to the Agency are in peril.

I said at the outset that I would not propose to you any solution. My purpose is to bring to your attention the Agency's perspective on the problem. I am convinced that the concerns I have enunciated should not lead to the conclusion that nongovernmental cryptologic endeavor must somehow be halted. I think such a step would be a disservice to everyone. Similarly, any restrictions on domestic dissemination of the fruits of such endeavors should be approached most cautiously and in a highly limited framework. With respect to the exports of technology and equipment, I have much less hesitation. I believe that the present regulatory framework should be strengthened with respect to the export of cryptologic equipment and technical information having a direct relationship to such equipment. At the same time it should be clarified (and will be) so as to leave unfettered the free flow of basic research and scientific information among scholars in different countries.

Were any kind of restriction to be placed on domestic dissemination of nongovernmental technical information related to cryptology, such restrictions, in my opinion, would have to meet several criteria, for both policy and legal reasons. Among these criteria are the following:

- The restriction should apply only to a central core of critical cryptologic information that is likely to have a discernable adverse impact on the national security.
- Law and regulations should make these criteria as clear as is possible without revealing information damaging to the national security.
- The burden of proof in imposing any restriction on dissemination should be borne by the government.
- There should be judicial review of any such government action, perhaps by a specially constituted court that could act under suitable security precautions, and the government should bear the burden of obtaining judicial approval of its action.
- There should be fair, full and prompt compensation for any company or person losing the economic benefit of information by virtue of governmentally-imposed restrictions on dissemination.

Whether the risks to the national security I have described today should lead to the imposition of any

additional government regulation is clearly a controversial question and one that remains to be fully examined by the Executive Branch, the Congress, and interested segments of the public. In my view, such examination should commence without delay and with the recognition that inaction is as much a choice as action in these circumstances. Any choice should be based on full consideration of all relevant information and views. In the coming months, NSA will be undertaking discussions with the industrial and scholarly communities for purposes of better understanding the diverse points of view to be found in the private sector and, it is hoped, of stimulating consideration of alternative possible solutions. I solicit your participation in this process.

That completed the formal remarks. At the January session there was no opportunity for questions. There were a few questions in the February one in Los Angeles; they were essentially non-controversial and simply sought clarification. I would not tell you that there was a great standing ovation or public outcry of support; on the other hand, the flow of mail on balance has been supportive and there has been a very wide ranging set of queries from people asking "How can we be of help?"

* * * * * * *

Here are the main points made by Admiral Inman in responding to questions from the audience.

On the subject of using contractors and giving them sensitive information...

I do not think there is any prospect of altering the increasing dependence on contractor personnel. There has been a substantial acceleration of our dependence on industry in many areas over the last several years as a direct fall-out of a conscious government decision to reduce the over-all size of management in the Sigint system. In the process we have had to move from doing perhaps 75 per cent of our research, development, and engineering in-house to a situation where now perhaps 85 per cent of that is done externally. There is at this point zero prospect of reversing that trend, notwithstanding some pretty hardy efforts to try. In fact, we are having a pretty difficult time in simply sustaining the floor that we have right now to avoid further erosion. I am reasonably confident that we are going to retain that floor, with perhaps a few gouges in it. But the prospect of substantially enhancing our ability to do these things it needs, thereby reducing this transfer of knowledge out to industry, simply is not going to exist.

One of the processes, though, that we are looking at in moving toward some improved control, or at least the prospect that we would go for increased control unless definite restraint is shown, is a hope that we can limit how much of that transfer of knowledge gets out into the public media. In tracing some of the worst publication that has occurred thus far, I do not find any sign of a direct transfer where someone who worked on projects here then consciously transferred that knowledge into the media, or into international symposia. A good deal of it appears to be secondhand.

There is a lot of bright work going on in the academic community as well as in industry, and I believe the danger is growing that they will reinvent things which have already been done here, and the fact that these techniques are seven or ten years old will not materially lessen the damage that could be done if they end up being transported to foreign cryptology.

On NSA's role in public cryptography...

(C) When I arrived July 1977 I found that the administration was embarked on a review of the whole question of communications security for the private sector and that there was a doctrinal approach which said that the government must undertake activity to make available protective measures in the private sector as a government responsibility, and that it would be intolerable for that to be done by an Agency which had signals intelligence as its primary mission. All kinds of attempts to educate people as to the underlying fallacies of that doctrine were unsuccessful, and the end result was a positive decision to move forward in creating a separate communications security responsibility within the Department of Commerce under the National Telecommunications Information Agency, which has been specifically tasked to make available to the private sector information and assistance in increasing communications security. We have set about trying to implement the decision in a

damage-limiting approach, recognizing that one would not be able to avoid all damage, and we have been reasonably successful. There have been a lot of very hard efforts, mostly by the S organization working at a whole variety of levels within NTIA, an organization which has some bright people who have proven to be understanding of a great many of our concerns.

(C) But there are several areas where there are issues that are unresolved. There is the question of who ought to develop the government's policy in the whole public cryptography area. Also closely related to that is the question of who develops export controls.

(S) It was with that policy dispute in mind, that I consciously went public, to remind those who were solely concerned about the protection in the private sector that there were indeed national security interests that warrant equal concern. I would prefer to get a solid decision inside the government rather than doing it by building public pressures, and hopefully a judicious mix of the two will be useful. I have some optimism that the Congress will weigh in very shortly to renew its interest, for it has been overwhelmingly responsive to our concerns.

On legislation...

I would tell you candidly that there is disagreement within the Agency over whether there should be legislation or not. There is one strong view that measures from the past really have been successful, and that the cost in publicity of getting legislation is so high that we should not take the risks. That view tends to evaluate what has happened in the public sector and decide "It isn't so bad after all," as compared to what might happen if we get into a public debate searching for legislation.

The primary opposing view is that we are on an upward trend of interest in public cryptography, that the commercial market is going to boom, and that is going to give substantially greater impetus unless there are legislative means for controlling it. And, given a general mood of support in the Congress, that we probably can get general legislation that would serve as a constraint.

The last remarks that I made in that speech, in fact, set out the basic framework that such legislation would undertake. It would specifically apply export controls, and it perhaps would set up a telecommunications security review body outside NSA — not governed here, but within the government — which would include at least some people with great depth of experience in Sigint as well as Comsec.

That Board would be a place where the public could come and make application, and if the Board decided to apply restrictions, there would be a mechanism for appeal externally to the Court that is set up to govern the new National Surveillance Act. It probably would be a feasible mechanism, but we must be concerned about the people who would not elect to go to the Board, who would elect to defy it and go ahead and publish.

Parallel to this public activity before friendly audiences has been some dialogue with the academic community. The General Counsel accompanied me for a session with some of the faculty at the University of California campus at Berkeley. It was not, at least at the outset, the friendliest gathering that I have encountered over the years, but I think on balance we drew some eventual substantial interest in our concerns. We certainly did not draw any overwhelming interest in legislation, but we did get, at their initiative, some discussion of the kind of legislation they could live with, if legislation were going to occur.

We have another session coming up in May — a symposium sponsored for us by the American Council on Education that a few of us will take part in with the presidents of a few universities, and the heads of Mathematics Departments and Computer Departments. Again it is more of the process of trying to understand what the worries are in the public sector about expanded control, and getting across to them why we view with alarm some of the unconstrained efforts which have continued in the public sector.

On public revelations about NSA...

We separately are examining a lot of these topics, in trying to do a zero-base review of anonymity, looking to find those elements of it which are essential to the performance of the Agency, and to reinforce those elements. Clearly, special collections operations, some of our sensitive overseas collection programs, require extraordinary endeavors to insure that they are not identified as signals intelligence collection operations.

On the other hand, I believed before I came — and that belief has been reinforced — that this is a mature workforce that can in a proper forum be identified as being employees of NSA without instantly throwing to the winds the security that has so well served the Agency over the period of its existence. There are some balancing concerns. There is Public Law 86-36, which has in the past been particularly helpful in dealing with Freedom-of-Information-Act requests and other things. And one therefore examines each step very cautiously, not wanting to run the risk that a court challenge, like this challence of *The Progressive Magazine* against the Atomic Energy Act, would lead to some striking down of those provisions which have

been so helpful for security. We will be proceeding as cautiously on that track as we have on this open dialogue. One step at a time.

I would expect to see some pronouncements with regard to things we do with respect to recruiting and other things in the very near term, in the next couple of weeks — permitting some additional things to be done that will make it easier to recruit talent. But there will not be a complete taking off of the wraps anytime in the near future. One step at a time.

On NSA anticipating the problem of public cryptography...

~~(C)~~ That's a question I probably had better duck, simply because I was not here for any part of it. From my very limited observation, I don't think there was any particular reason to anticipate some of the academic interest in the cryptomath area. On the other hand, computer security and the security of information and data banks has for the last few years been a growing cause of public concern, and all you need is another episode of transferring funds to a Swiss bank to turn that into one that is going to merit a lot of attention.

~~(C)~~ We are walking along the edge of a different kind of problem, and that is the danger that political opportunism will lead to substantial exposure of specifics of foreign collection activity in this country — and, in turn from that, a great outcry for rapid increase in efforts in the private sector. That political opportunism seems to draw its strength from a recognition that the Administration is in a difficult position, that security constraints keep it from advertising what it has done, and therefore it can easily be displayed as being weak or disinterested in intelligence activity that is being conducted by foreign countries within these shores.

~~(C)~~ The facts of life are that there has been foreign-intelligence collection activity in this country, at least since it became a republic, just as we have conducted foreign-intelligence activity in all sorts of other places around the world, and, in the nation's interest, we will continue that activity. The electronic age has made it much easier to do that surreptitiously. All of that needs to be taken into consideration in the national telecommunications programs of the country. It certainly has been taken into consideration in the programs to protect government communications. The underlying question is what responsibility the government has in the private sector, in the absence of a clearly demonstrated concentration on collection against that private sector.

~~(C)~~ The decision to try to do something, but not to do very much, has probably increased the opportunity for a political opportunist to draw a lot of banner headlines and some good prime-time television coverage. And I would tell you that that probably is one of the greatest hazards we face in the next few months.

During his 27-year naval career, Admiral Inman has held a number of executive positions in the intelligence field. Before his present assignment he was Vice Director for Plans, Operations, and Support for the Defense Intelligence Agency. He has served as Director, NSA/Chief, CSS since July 1977.