Description of document:	Article: NSA Comes out of the Closet: The Debate over Public Cryptography in the Inman Era, Cryptologic Quarterly, Spring 1996
Requested date:	17-May-2021
Release date:	26-May-2021
Posted date:	10-January-2022
Source of document:	National Security Agency ATTN: FOIA/PA Office 9800 Savage Road, Suite 6932 Ft. George G. Meade, MD 20755-6932 Fax: 443-479-3612 Submit A FOIA Request Online

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

FOIA Case: 111902
26 May 2021

This responds to your Freedom of Information Act (FOIA) request of 14 May 2021, which was received by this office on 17 May 2021, for "A copy of the article: NSA Comes out of the Closet: The Debate over Public Cryptography in the Inman Era, Cryptologic Quarterly, Spring 1996." Date Range of Requested Documents: 1996. Your request has been assigned Case Number 111902. There are no assessable fees for this request; therefore, we did not address your fee category.

Your request has been processed under the FOIA and the document is enclosed. Certain information, however, has been protected in 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 Subparagraphs (b) and (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)).

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 disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Commercial and financial information that is privileged or otherwise confidential has been protected, pursuant to the fourth exemption of the FOIA.

In addition, information has been withheld from the enclosure pursuant to the fifth exemption of the FOIA. This exemption applies to inter-agency or intra-agency memoranda or letters that would not be available by law to a party other than an agency in litigation with the agency, protecting information that is normally privileged in the civil discovery context, such as information that is part of a pre-decisional deliberative process, attorney-client privileged information, and/or attorney-client work product.

Finally, personal information regarding an individual has been withheld from the enclosure in accordance with 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

Since these withholdings may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

  NSA/CSS FOIA/PA Appeal Authority (P132)
  National Security Agency
  9800 Savage Road STE 6932
  Fort George G. Meade, MD 20755-6932

  The facsimile number is (443)479-3612.
  The appropriate email address to submit an appeal is FOIARSC@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov
877/684-6448
202/741-5769

Sincerely,

RONALD MAPP
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encl:
a/s

NSA Comes Out of the Closet: The Debate over Public Cryptography in the Inman Era (U)

[redacted] (b)(3)-P.L. 86-36

(U) From the adoption of the Data Encryption Standard (DES) to the end of the Inman era, various policies dealing with public cryptography were suggested and attempted. Opinions within NSA ranged from a desire to exert complete control over all public cryptography, to a belief in a more laissez-faire approach to the subject. In the end, NSA attempted to navigate through public exposures and obtain a policy which provided some protection for traditional national security concerns on public cryptography.

(U) The policy decisions faced by NSA from 1976 to 1981 still present themselves today. What should be NSA's responsibilities and goals in the movement of the American public to strong cryptographic systems? Should NSA be an active or passive participant? Should it help or hinder the effort? This paper examines how these questions were discussed and answered when the issues first presented themselves.

DEFINITIONS

(U) In order to intelligently discuss the evolution of the National Security Agency's policy regarding public cryptography, it is first necessary to define the terms under consideration. Specifically, what exactly is meant by "public cryptography" and how does it differ from other cryptographic efforts? Fortunately, the 1978 National Security Agency Scientific Advisory Board (NSASAB) Task Group on Public Cryptography proposed a definition which retains its usefulness today and will therefore be used throughout this discussion.

(U) To begin, the Task Group categorized two different types of information: National Security Information and National Interest Information. National Security Information is defined as official information which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States. National Interest Information, on the other hand, involves information (not national security information) that is either deemed by national authorities to be important to national policy interests (e.g., dollar valuation data, agricultural commodity data) or protected by Congress in the public interest (e.g., Privacy Act material).[1]

(U) Next, the Task Group structured its definition based on three criteria: (1) the types of information being protected; (2) the threat against which the protection is being directed; and (3) the type of protection provided. Using these criteria, Public Cryptography can be defined as the protection of data that is neither National Security nor National Interest Information from exploitation by unauthorized groups or individuals through the application of cryptography as deemed necessary by the concerned parties.

This definition should contrasted to with National Security Cryptography, which protects National Security Information from exploitation by foreign powers or other groups with interests opposed to those of the United States, and employs cryptography pursuant to the orders of an assigned executive agent. Likewise, it differs from National Interest Cryptography, the final category of cryptography defined by the 1978 Task Group. National Interest Cryptography, as its name implies, involves the protection of National Interest Information from exploitation by unauthorized groups or individuals, except as authorized for legal purpose on the part of the government. National Interest Cryptography, like National Security Cryptography, depends on standards set forth by an assigned executive agent.[2]

(U) It is important that this definition of public cryptography center on how a system is used, as opposed to technical properties which it might possess. There is no implied cryptographic weakness or limitation in this definition of Public Cryptography, nor is there necessarily recognition that the algorithms used for each type of cryptography need differ. As an example, the DES algorithm, originally conceived for use in a National Interest Cryptography system, has been used for both National Security Cryptography and Public Cryptography.

THE CREATION OF THE DATA ENCRYPTION STANDARD

(U) The 1965 Brooks Act gave the National Bureau of Standards (NBS) the authority to establish standards for the purchase and use of computers by the federal government. In 1968, Dr. Ruth Davis, then head of the Institute for Computer Sciences and Technology at the NBS, investigated the need for computer security within the government. Aided by the 1974 Privacy Act, which further emphasized that personal government records needed to be protected, NBS concluded that it was necessary to develop a government-wide standard encryption device to provide adequate security for unclassified computer data. Without a single standard, NBS argued, the purchase of computer equipment and the necessary sharing of data between agencies would be complicated. Each agency would be dependent on its own enciphering system, making it difficult for the NBS to adequately perform its statutory tasks.[3]

~~(S-CCO)~~ In 1972, Dr. Davis approached NSA with the concept of a standardized encryption algorithm. Meeting with NSA individuals from Research and Engineering (R5), she was able to secure a Memorandum of Understanding between NBS and NSA on computer security, to include cryptography. By April 1973, it was decided that NBS would use the *Federal Register* to solicit the commercial sector for encryption algorithms. NSA would evaluate the quality and the security of the algorithms submitted and, if no acceptable algorithm were found, submit its own entry.[4]

~~(S-CCO)~~ The NBS advertisement for encryption algorithms appeared in the *Federal Register* on 15 May 1973, but few responses were received. By July, NSA had started to develop its own encryption algorithm for the NBS. At that time, Howard Rosenblum, then

deputy director of research and engineering, discovered that Walter Tuchman of IBM was working on an encryption chip which could be used for general-purpose computing. IBM had developed an encryption algorithm called LUCIFER for Lloyds Bank of London in 1971, and Tuchman had been working on improving the algorithm for general use.[5] The new version, DSD-1, appeared to be a good starting point for the NBS standard. In September 1973 Tuchman received [redacted] and he started work with NSA analysts to examine DSD-1.[6]

(U) Cooperation by NSA with the NBS standard creation process was a significant change from traditional agency operations. NSA had viewed itself as the sole cryptologic authority in the United States, and the NBS effort eliminated that monopoly. However, cryptology was already being discussed by more and more commercial firms.[7] Supporting DES was an important policy decision made by the NSA, and it would force NSA to further define its role in the development of national interest and public cryptography.

~~(S-CCO)~~ The decision by NSA to support the NBS effort was a difficult one, [redacted]

[redacted] The need for an unclassified government algorithm to be used by both the federal government and commercial firms to protect computer information was present, and the NBS effort was viewed as offering a possible solution to this problem.

[redacted]

~~(S-CCO)~~ Tuchman continued to work with NSA to develop a secure version of DSD-1. NSA COMSEC agreed to evaluate the algorithm and to make the algorithm secure against

all attacks except exhaustion of key variables. [redacted] and reducing IBM's key bit length from 64 to 48.[12] In June 1974 NSA and IBM agreed on an improved 56-bit key version of DSD-1 with 16 internal rounds and secure S-Boxes. This new version was offered to NBS by IBM in August 1974.[13]

THE DES CONTROVERSY

(U) On 17 March 1975 NBS published in the *Federal Register* its intention to use IBM's algorithm as a federal standard for data encryption. This initiated an acrimonious battle between NSA and academicians that would highlight the need for a formal NSA policy on public cryptography. The debate, prominently featured in the media, centered on NSA's role in the development and use of public cryptography.

(U) Almost immediately after NBS announced its intention to certify DES, academicians started an intense effort to replace DES with a system they viewed as more secure. Professor Martin Hellman from Stanford University was one of the first and most vocal critics of DES. In May 1975 Hellman started a dialogue with NBS in which he complained that DES provided little security and that it would soon be rendered useless as technology improved. In addition, Hellman and other academicians were suspicious of the presence of a trapdoor in the code.[14] This fear was increased by NSA's refusal to provide any comment on how the S-Boxes in the algorithm were chosen. Academicians worked furiously analyzing DES in an attempt to demonstrate that a more secure algorithm was needed.

(U) On 3 April 1976 the DES controversy spilled into the popular media. David Kahn, a journalist best known for his history of cryptology, *The Codebreakers*, stated in the *New York Times* that DES "has been made just strong enough to withstand commercial attempts to break it, it has been left just weak enough to yield to Government cryptanalysis."[15] Playing on the fears of a post-Watergate nation that saw NSA as being interested in tapping the lines of domestic targets, Kahn warned that "recent history has shown how often an agency exercises a power simply because it has it."[16]

(U) In an attempt to reaffirm the security of DES, NBS announced that it would sponsor two workshops to discuss DES. The first occurred in August 1976, and it investigated the resources necessary to build a hardware device capable of breaking DES. Various figures were advanced as to the cost of such a machine. Hellman suggested that one could be built within two years at a cost of $9 to $11 million and that such a machine could solve a single message in approximately twenty years. By 1978, Hellman would theorize a machine that would cost $4.2 million and be capable of 100 solutions per day. Less optimistic cryptanalysts, such as Tuchman from IBM, saw a machine that could be built by 1990 which would cost $72 million and solve one DES key per day. In any event,

NBS responded that it would reevaluate the algorithm every five years to insure that technology did not significantly degrade the security provided by DES.[17]

(U) The second NBS workshop on DES was held in September 1976. While the first workshop was dominated by hardware specialists, many with firms that had a financial interest in DES, the second workshop involved a more independent group of software specialists. Their opinions were not nearly as optimistic as those expressed in the first workshop, and their findings were well published in many of the technical journals. They believed that the security provided by the DES algorithm would degrade to unacceptable levels within the very near future. The two most important points of discussion were the classified criteria for the creation of the S-Boxes and the reduced 56-bit key size. Academic opposition to these features was widespread and intense.[18] Efforts were made by academics to provide NBS with "neutral" experts who could act as a counterweight to the perceived pressure that NSA was exerting on the process.[19]

(U) On 15 January 1977 NBS published the DES algorithm and announced that DES would become the U.S. government standard effective July 1977. It would be used as the standard national interest cryptographic system, in addition to being available to any domestic individuals or institutions that wanted to employ it for public cryptography. While NSA had enjoyed some success in obtaining the acceptance of DES as a standard by the NBS, the result was hardly encouraging for the Agency. The field of cryptology was being discussed in the open press as never before, and DES provided an excellent cryptologic training tool. Many academicians were becoming openly hostile to NSA, and they viewed DES as a tool for government abuse. Furthermore, the role of NSA in supporting DES was anything but clear. While NSA was the executive agent for national security cryptology, it was not apparent who was the executive agent for National Interest Cryptography.[20] Many issues raised by DES were still unanswered, and the climate created by NSA's support of DES insured that any policy decisions made by NSA would be met with the strictest public scrutiny.

A NEW DIRECTOR

(U) On 5 July 1977, Vice Admiral Bobby Ray Inman replaced Lieutenant General Lew Allen Jr. as the director of NSA. Inman had held a variety of intelligence posts within the Defense Department, including director of Naval Intelligence and vice director of Plans, Operations, and Support at the Defense Intelligence Agency. He came to NSA with a good deal of experience in dealing with Congress, and he was a veteran of several congressional investigations while serving his position in Naval Intelligence. Inman was often described as a skilled diplomat, and it would be these skills which were most needed in the debate over public cryptography.

(U) Upon becoming DIRNSA, Inman was quickly forced to deal with several public cryptography issues. Various crises, generally well covered by the media, arose regarding NSA policy on secrecy patents, academic research, cryptographic research sponsored by other government agencies, export control, and support for DES. These episodes focused

NSA's attention on the issue of public and national interest cryptography, and Inman would play a leading role in the development and implementation of NSA policy.[21]

NATIONAL SCIENCE FOUNDATION

(U) As the discussion of DES and cryptology in general became more common in the academic world, the National Science Foundation (NSF) soon found itself presented with funding requests for cryptologic research. The response of NSF to these requests would dominate NSA/NSF relations.

(U) During the early 1970s, there had been sporadic contact between NSA and NSF to coordinate cryptographic research. In 1975 the NSF contacted the NSA to determine if federal agencies other than NSA were allowed to support cryptographic research. After consulting with NSA, NSF assistant general counsel Jesse E. Lasken found that no prohibition on cryptologic research funding by NSF existed. NSF did submit cryptologic research proposals to NSA at that time, but NSF viewed NSA simply as an advisor on the technical merits of the proposals.[22]

~~(S-CCO)~~ In November 1976 Hellman published "New Directions in Cryptography" with graduate student Whitfield Diffie. This first public work on the topic of public-key cryptography was supported by NSF funds and discovered results that were both known and classified by NSA. In response to this, NSA sent Cecil Corry, assistant deputy director for communications security, and David Boak to meet with Dr. John Pasta, director of NSF's Division of Mathematical and Computer Sciences, and Dr. Fred Weingarten, the special projects program director of NSF's Division of Computer Research. During this 20 April 1977 meeting, Corry stressed that NSA required the ability to review NSF grants for both technical and security considerations. Believing Pasta to be in basic agreement with this position, Corry later thanked Pasta for his "willingness to cooperate with [NSA] in considering the security implications of grant applications in this field."[23] Pasta pledged no such cooperation, insisting instead that NSA could review NSF proposals for their technical merit only.[24]

~~(S-CCO)~~ NSF continued to fund advanced research in cryptology. An April 1977 research paper was especially troubling to NSA. The paper, "On Digital Signatures and Public-Key Cryptosystems," was authored by Dr. Ronald Rivest of the MIT Computation Laboratory. This paper expanded the public-key idea first proposed by Hellman and represented an important breakthrough in public cryptography. The research was supported by grants from NSF and the Office of Naval Research (ONR), and it duplicated NSA research results obtained more than five years earlier. NSA did not receive any indications that this research was occurring until May 1977 when it received a copy of the published paper.[25]

~~(S-CCO)~~ NSA was not sure how to react to the MIT paper. Various policy directives were contemplated. Some elements within the Operations Directorate urged that the paper be seized and classified since it was supported in part by Department of Defense

funds.[26] Others suggested a general application of the International Traffic in Arms Regulations (ITAR) to stop the publication of this type of cryptologic research.[27] Eventually NSA officials sought additional information on the MIT grant from Pasta at NSF. The abstract of the Proposed Statement of Work submitted to NSF by Rivest was exceptionally vague, and NSA officials concluded that it would have been impossible from the abstract alone to determine that Rivest's research would involve cryptographic results. NSF had not intentionally broken its commitment to involve NSA in cryptographic research grants.[28] Inman then made a personal appeal to Rear Admiral Robert Geiger, ONR, Chief of Naval Research, to coordinate all future cryptographic research with NSA. Pointing out that the MIT grant simply duplicated established classified results, Inman made a strong case for NSA oversight.[29] This argument would later be expanded and developed into one of the principal goals of NSA public cryptography policy.

A LETTER TO IEEE

(U) ~~(FOUO)~~ The proliferation of public articles on cryptology sparked strong reactions from some within the NSA. Joseph A. Meyer, an NSA employee in the Operations Directorate (P13), wrote several in-house summaries of public cryptographic work being done. These papers contained harsh criticism of NSA's unwillingness to take direct action against these publications under the authority of ITAR.[30] There was some disagreement within NSA regarding ITAR usefulness against journals and research papers. After Meyer complained that NSA was using an informal prepublication review rather than a formal ITAR classification review with articles in the journal *Cryptologia*, Norman Boardman, Chief of the Policy Staff, responded:

> D4 [Policy Staff] does not agree that the ITAR can be used to control publications of cryptologic data. As noted in the ITAR, under 125.11 General Exemptions (1) (ii), unclassified technical data available by subscription or purchase can be exported without a license. There is no requirement under ITAR for a publisher to submit material for classification review purposes.[31]

(U) Although Meyer found some disagreement with his position within NSA, he continued to issue warnings on papers and conferences available to the public which dealt with cryptology. When the Institute of Electrical and Electronic Engineers (IEEE) Information Theory Group called for papers on encryption to be presented at the 1977 International Symposium in Ithaca, New York, Meyer felt that he had to share his ITAR concerns with IEEE. Acting on his own, Meyer penned a detailed note to E. K. Gannet, staff secretary of the IEEE Publications Board. In the 7 July 1977 letter to Gannet, Meyer pointed out that encryption and cryptologic and related systems were covered by ITAR and that prior government approval would be necessary for the publication of many of these papers. Meyer also noted that IEEE was supplying this information to foreign nationals, specifically from the Soviet Union.[32] Gannet replied, much as NSA's Policy Staff had, that their publications were exempt from ITAR restrictions. Gannet did agree that the IEEE/USSR exchange needed to be examined and promised to bring Meyer's concerns to the appropriate IEEE policymakers.[33]

(U) Meyer's letter made an impact on the IEEE. The director of Technical Activities of the IEEE, Dr. Nirendra Pundit, decided to circulate the Meyer letter to the members of the Information Theory Group. Pundit stated that he did not agree with Meyer's interpretation of ITAR, but Pundit believed that the Information Theory Group should be aware of the situation. The Information Theory Group attempted to find a legal opinion on ITAR applicability to conference papers, but it could find no lawyer willing to provide a definitive statement.[34]

(U) Meyer's letter also made an impact on the press. On 15 September Deborah Shapley, a reporter with *Science* magazine, contacted Meyer to question him about the letter. Although Meyer had written the letter on plain stationery with no indication of his place of employment, it was soon discovered that he was connected with NSA. Shapley subsequently published an article in *Science* magazine claiming that NSA was currently involved in a policy of harassing scientists and impeding research in public cryptography.[35] Congressional reaction to the article was swift, and both the House and Senate presented several inquiries to Inman.[36]

(U) The International Symposium on Information Theory was held as scheduled at Cornell University in October 1977. The press attended the conference in force, prepared for NSA action to prohibit discussion of some of the research papers. The conference was tense at times, as Hellman announced that he would present research completed by his graduate students to shield them from any litigation that NSA might attempt. Discussion centered on an NSA conspiracy involving the creation of an intentionally weak DES, followed by NSA strong-arm tactics against NSF and those involved in public cryptography research. Reacting to this public relations nightmare, NSA spokesman Norman Boardman issued the standard Agency response that "neither he nor any other employee of the Agency could comment in any way on the accusations made by the scientists."[37]

SENATE HEARINGS

(U) Public cryptography issues were overwhelming Inman and NSA. DES, NSF, and the Meyer letter had resulted in significant public attention to the field of cryptography. Claims of NSA wrongdoing were taken seriously by NSA's congressional oversight committees, and by November 1977 the Senate Select Committee on Intelligence was investigating the charges against NSA.

(U) The Senate committee recognized the dilemma that NSA faced over DES and public cryptography. While NSA was tasked with maintaining a strict monopoly on all cryptologic activity in the government, it understood the legitimate public needs for data security. The Senate committee focused on two major sets of allegations against NSA. First, they examined the role of NSA in the development of DES. Specifically, they investigated the claims that

> NSA, under the guise of testing the mathematical formulae submitted to NBS for consideration as a Data Encryption Standard, "tampered" with the final algorithm in order to weaken it and create a "trapdoor" which only the NSA could tap.
>
> NSA forced IBM to compromise the DES's security by reducing the key size used in the encryption and decryption process.
>
> DES failed to allow for future technological advancements which will permit successful brute force attacks within the next several years.[38]

(U) The Senate committee interviewed numerous people from IBM and NSA in order to determine how much impact NSA had on the design of DES. In their investigation, the Senate committee found no basis for any of the allegations. It confirmed that

> 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.[39]

In addition, the Senate committee concluded:

> The overwhelming majority of scientists consulted felt that the security afforded by the DES was more than adequate for at least a 5-10 year time span for the unclassified data for which it will be used.[40]

~~(TSC)~~ While the Senate may have overstated IBM's primacy in the development of the DES, their reliance on the claim that DES would be adequate for the five-to-ten-year time span was justified. DES has been reviewed every five years since its adoption. It was easily recertified in 1982. In 1987, NSA proposed a new Commercial COMSEC Endorsement Program that would provide algorithms to replace DES. This suggestion was not well received, especially by the financial community which had come to rely on DES, and DES was recertified as providing sufficient public cryptographic protection in 1987 and 1992.[41]

(b) (1)
(b) (3)-18 USC
(b) (3)-P.L. 8

[redacted] the algorithm generally served its role as a strong, general-purpose encryption system for public and national interest cryptography.[42]

(U) The Senate committee also saw the need to examine the claims that NSA was involved in harassing scientists working in the field of public cryptography. Indications of this harassment included the NSA/NSF dispute over the NSF's role in funding cryptographic research and the Meyer letter to IEEE expressing his opinion that some public dissemination of cryptographic research was not allowable under ITAR. The Senate found that most of the accusations leveled in the press were inaccurate. Scientists such as Hellman and Rivest, who were reported as the subjects of harassment, noted that NSA had made no efforts to harass them. Likewise, NSF officials did not view relations with NSA as limiting their freedom to support cryptographic research. However, all parties involved were in agreement that the uncertainty and ambiguity in the current understanding of the applicable laws created a poor environment for everyone. The Senate committee concluded:

> 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;
>
> The NSF should decide what authorities and obligations it has to consider the national security implications of grant proposals;
>
> The NSF and NSA should initiate efforts to reduce the ambiguity and uncertainty which surrounds the granting of funds for research in public cryptology;
>
> The NSF and NSA 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 and cryptanalysis.[43]

~~(S)~~ An unclassified summary of the report, which did not include some of the more specific details of NSA's involvement with DES, was made available to the public in April 1978. It was met with mixed reactions. Some accepted the results of the Senate committee investigation, while others chose to focus on "unanswered questions" about NSA's role in public cryptography.[44]

(U) Clearly, the Senate report was viewed by NSA as a positive step in addressing its negative press image. The committee had cleared NSA of any wrongdoing in NSA's support of DES, and it had countered the press reports of NSA intimidation against NSF and public researchers. In addition, the report acknowledged some of NSA's concerns over public cryptography and attempted to address them. For NSA, now was the time to work quietly on developing a comprehensive policy to deal with the development of public cryptography.

ITAR

(U) NSA's success in containing the public cryptography issue was short lived. After the publicity of the Meyer letter, Dr. Frank Press, presidential science advisor, suggested to Inman that NSA contact the Department of Justice for advice on the application of ITAR.[45] As stated by Meyer's letter to IEEE, ITAR could be viewed as requiring authors and publishers to submit public cryptography papers to NSA for classification determination. If this were so, NSA could rely heavily on ITAR to reduce the publications on public cryptography.

(U) ~~(FOUO)~~ Specifically, NSA wanted clarification on three main points. First, did ITAR require authors who wished to publish unclassified technical public cryptography data to submit their articles to the NSA prior to dissemination? Next, were such authors obligated to notify publishers and other recipients that dissemination to foreign nationals was prohibited unless the paper was examined for ITAR compliance? And finally, would an individual be prohibited from discussing unclassified technical data at a symposium if foreign nationals were present?[46] An affirmative answer on any of these would provide NSA with significant leverage in dealing with public researchers.

(U) In May 1978 the Justice Department surprised NSA with the following response:

> It is our view that the existing provisions of the ITAR are unconstitutional insofar as they establish a prior restraint on disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector.[47]

(U) The Justice Department based its conclusion on several factors. First, ITAR was an executive branch order. The Justice Department felt that additional legislative authorization would be needed to provide for prior review of cryptographic material for export. In addition, the restrictions would need to be much more narrowly constructed to justify prior constraint. This would force NSA to specify clearly what the national security threat was and to identify for prior review only those items designated by that threat. Finally, prior restraint would require judicial as opposed to institutional review, with the burden of proof on the government agency seeking to impose secrecy. The Justice Department noted that such a system of prior restraint could be established, but the current rules of the ITAR did not meet the constitutional requirements.[48]

(b) (5)

(~~FOUO~~) NSA had strong disagreements with the Justice Department opinion. Expecting guidance on how to effectively employ ITAR, NSA was not prepared for such a complete repudiation of ITAR safeguards. In response,

(U) ~~(FOUO)~~ NSA soon received important support in its disagreement over ITAR constitutionality. The State Department, which oversaw the United States Munitions List of items restricted by ITAR, also expressed its disagreement with Justice's opinion. State noted that ITAR had always been applied narrowly to "technical data relating to the manufacture, operation or maintenance of arms, ammunition, and implements of war."[51] State asserted that while ITAR itself was constitutional, its application to public cryptography was perhaps unclear. For this reason, State suggested that an interagency study, involving State, NSA, Justice, and other federal agencies involved with public cryptography, was the best context to develop guidelines to insure that ITAR was being constitutionally applied.[52]

~~(FOUO)~~ The Justice Department agreed to work within the interagency format. Eventually, the group produced new instructions for applying ITAR to public cryptography. These instructions included a narrow definition of the technical data under control, emphasizing that basic scientific or theoretical information was not covered by ITAR restrictions. In addition, a procedure for voluntary review of noncommercial exports was created. This would allow researchers who felt that their work might be covered by

ITAR to quickly receive an opinion from the State Department.[53] These clarifications were later published in a Munitions Control Newsletter, and the control of technical data has since been upheld in a variety of judicial decisions.[54] Thus, while NSA's initial hopes for a more expansive reading of ITAR went unrealized, the basic protection provided by ITAR remained.

SECRECY PATENTS

(U) Another tool which had been useful in the NSA's public cryptography efforts was the secrecy patent. Under the 1951 Invention Secrecy Act, any application for a United States patent on an invention that might impact on national security interests was investigated by the Department of Defense. For cryptologic inventions, the patent application was routinely passed to NSA for evaluation. If NSA determined that the invention could be harmful to national security, it could recommend to the patent office that a secrecy patent be issued. This would prevent the inventor from disclosing any aspect of his invention to others. While the Invention Secrecy Act did allow the inventor to receive compensation for any damage suffered by reason of the imposition of the secrecy order, the Act also effectively removed the invention from the market.

(~~S-CCO~~) Within NSA, patent applications were received by the NSA patent attorney and distributed for comment to those offices with expertise on the subject matter. In December 1977 one such application was received involving a "Digital Data Enciphering and Deciphering Circuit and Method" created by Dr. George Davida of the University of Wisconsin. The application was first evaluated by the S COMSEC Organization, which believed the invention to be unclassified. However, the application was then evaluated by the P SIGINT Organization, which asked that the "non-linear means and usual Linear Recursive Sequence (LSR) shift register" be sufficient cause to classify the invention at the SECRET level. The P Organization opinion was eventually forwarded to the DoD, and in April 1978 a secrecy order was placed on Dr. Davida's patent.[55]

(U) Once again, NSA had opened itself up to considerable public criticism on its public cryptography policy. The news of Dr. Davida's secrecy order was reported by *The New York Times*, *Washington Post*, and *CBS Evening News*, all of which noted that the invention had been supported in part by the National Science Foundation. Dr. Davida vowed to appeal the secrecy order, commenting harshly on what he perceived to be NSA's attempts to limit free speech and interfere with public research on cryptology. Amid several congressional inquiries, NSA reevaluated its decision to request a secrecy order on Davida's patent application. Eventually, NSA recommended the secrecy order be rescinded, and by June the Patent Office informed Davida that his patent no longer contained the secrecy order.[56]

(U) The Davida episode demonstrated to Inman that the present method of allowing "middle management" to request secrecy orders was seriously flawed. In response, Inman initiated a new procedure such that any requests by NSA middle managers to impose a

secrecy order would be reviewed by a senior team headed by the NSA general counsel.[57] Inman hoped that this new procedure would calm congressional and public criticism.

~~(S)~~ Inman's optimism proved to be unwarranted. In April 1978 a patent application made by Carl Nicolai for a speech scrambling device was evaluated by the NSA using Inman's new criteria. Once again, there was disagreement between NSA directorates. Neither Research and Engineering nor COMSEC believed that Nicolai's invention should be classified. Howard Rosenblum, DDC, noted that Nicolai employed "a sophisticated use of well-known, open-source techniques" of spread spectrum technology and that "so many unclassified spread spectrum systems are already in the public domain that it is too late to try to close the door by imposing secrecy orders based solely on the fact that the system uses spread spectrum techniques."[58] However, Operations argued that a secrecy order was indeed warranted for this potentially dangerous invention. Inman decided to "err on the side of national security," as he explained it, and he requested a secrecy order on the Nicolai patent.[59]

(U) Nicolai immediately sought the assistance of Senator Warren Magnuson (D-WA), a friend of the family. Nicolai noted the many hours and dollars put into this invention and stressed his commercial rights to market the device. Pressure from Magnuson and the press once more caused NSA to reevaluate its secrecy order request, and by October NSA had called for a recision of the order. NSA asserted that its original justification was based on the theoretical operation of the device, and it later removed the call for a secrecy order once the practical limitations of the device were investigated.[60]

(U) Opposition to NSA's use of the Invention Secrecy Act represented a recognition by Congress and the public that public cryptography was no longer an issue that should be dominated solely by national security concerns as pronounced by NSA. Like NSA's attempted use of ITAR, the use of secrecy orders to prevent the spread of public cryptography was being limited. New concerns involving personal privacy and commercial opportunities were quickly clouding NSA's responsibilities for public cryptography.

A NEW DIRECTIVE: PD-24

(U) On 16 November 1977 the White House attempted to answer some of the questions as to NSA responsibility for public cryptology. Presidential Directive 24 (PD-24) instituted a new telecommunications protection policy in which national security cryptography was separated from both national interest and public cryptography. The new policy provided the following instructions:

> The Secretary of Defense shall act as the Executive Agent for communications security (COMSEC) to protect government-derived unclassified information which relates to national security. COMSEC is concerned with protective measures designed for the security of classified information and other information related to national security.

> The Secretary of Commerce shall act as the executive agent for communications protection for government-derived unclassified information (excluding that relating to national security) and for dealing with the commercial and private sector to enhance their communications protection and privacy.
>
> It is recognized that there will be some overlap between the responsibilities of the executive agents in that Defense will continue to provide some non-cryptographic protection for government-derived unclassified information as it does now, and Commerce will have responsibilities in commercial application of cryptographic technology. The Subcommittee [of the National Security Council Special Coordination Committee] will review such areas on a case-by-case basis and attempt to minimize any redundancies.[61]

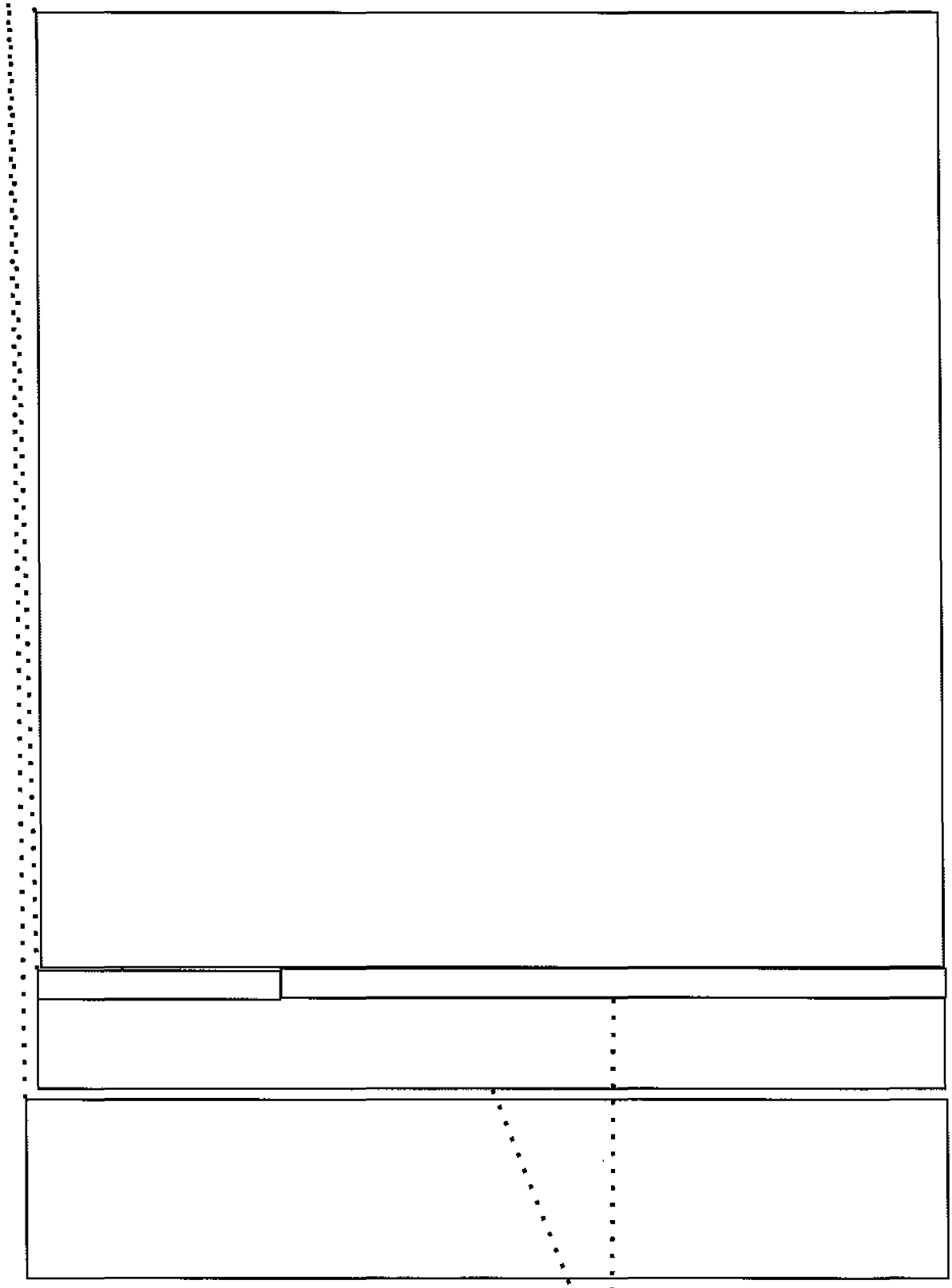
(U) Clearly, the NSA monopoly of cryptographic responsibility within the U.S. government had ended. The National Telecommunications and Information Administration (NTIA), a part of the Commerce Department, was now responsible for national interest and public cryptography. Whereas NSA viewed public cryptography with the maxim "the less said, the better," the NTIA would encourage public research and publicize the results. Understandably, NSA was uncomfortable with the new arrangements.

~~(S)~~ As NTIA attempted to develop a strategic plan for implementing PD-24, it faced strong opposition from NSA. Several issues immediately presented themselves as areas of overlap which required resolution. First, NSA questioned the role of the NTIA in the development of cryptographic export policies. NTIA asserted that it should be an equal partner with NSA in those aspects of export control policies which affected domestic public cryptography policies. NSA, however, believed that it retained primary authority for cryptographic export controls. While it saw the need to consult NTIA on issues which might affect domestic use of public cryptography, NSA believed the national security considerations of export controls were paramount.[62]

~~(S)~~ NSA also objected to NTIA's role in developing a policy for nongovernmental research. NTIA believed it was tasked with formulating a national policy balancing the public right to pursue independent research on cryptography with national security concerns. NSA saw this as an overly broad assumption of power by the NTIA. To NSA, NTIA was restricted to only those actions necessary for NTIA to accomplish its goal of assuring that adequate telecommunications protection was available for selected U.S. government, contractor, and private sector elements.[63]

(U) (~~FOUO~~) PD-24, far from clarifying NSA's role in public cryptography, instead added additional doubt and confusion. Prior to PD-24, NSA had been attempting to balance the national security equities involved in public cryptography. Now NSA was suddenly forced to consider commercial needs as stated by the Commerce Department. In general, NSA attempted to read NTIA's role under PD-24 as narrowly as possible, while simultaneously emphasizing its own national security obligations.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

INITIAL POLICY

~~(S-CCO)~~ With a growing number of public cryptography issues making their way into the press, Inman believed that it was necessary to examine NSA's views on the matter and develop an overall policy to address NSA concerns. Prior to Inman, NSA had a fairly limited policy on public cryptography. The major objectives of this early policy included

> Achieving the maximum commonality possible in the [redacted] policies on public release of cryptologic information;
>
> Encouraging U.S. authors and technical writers on cryptologic subjects to submit manuscripts for review by NSA;
>
> Identifying and if possible curtailing non-NSA research in cryptology funded by the [U.S. government] which results at times in the open publication of cryptologic information.[68]

~~(S-CCO)~~ In response to the perceived lack of an overall NSA policy, several groups discussed what actions NSA should take with respect to public cryptography. An initial gathering was hosted by Lowell Frazer, a COMSEC office chief, in May 1978. This informal gathering consisted primarily of technicians from DDO, DDR, and DDC. A consensus was formed on several issues. First, it was agreed that nothing presently published in the open press on public cryptography had a significant effect on current NSA activities. Next, it was argued that while NSA should discontinue its peer review of NSF grants, it should become the final authority for all cryptologic research within the Department of Defense. Finally, it was stated that NSA had excellent ties to the academic world, and it would be possible for NSA to stay abreast of any public research in the field of cryptography. Thus, the group determined the best policy was a "hands-off" approach to academic efforts and complete control of DoD cryptologic research.[69]

~~(C)~~ Other groups were not so optimistic. Several in DDO viewed the present situation as ripe for disaster. This group believed that new legislative initiatives, in addition to a strengthening of ITAR and Secrecy Patent Law, were necessary to combat the increasing discussion of public cryptography. Furthermore, those who believed otherwise were seen to "have [their] head[s] in the sand."[70]

(b) (5)

~~(C)~~ In July 1978 Inman asked his general counsel, Daniel Silver, [redacted]

[redacted]

[redacted] The directorates were tasked with providing additional comments and recommending an Agency policy.[71]

[redacted]

The Director has approved Option 1, the seeking of new legislation to control dissemination of non-governmental cryptologic information. [redacted]

[redacted]

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

NSA SCIENTIFIC ADVISORY BOARD REPORT

~~(C)~~ In December 1977 the NSA Scientific Advisory Board (NSASAB) had established a Task Group on Public Cryptography. Because NSA's role as the single government authority on cryptography had come into question, the NSASAB believed it should provide information and options to Inman regarding public cryptography. Specifically, the Task Group was to explore

> (a) NSA's role in public cryptography;
>
> (b) NSA's proposals for the best means of satisfying the technical, operational, and organizational requirements to effect public cryptography;
>
> (c) possible changes in NSA's liaison and technical cooperation with governmental and non-governmental groups responsible for the several aspects of public cryptography;
>
> (d) a clear delineation of NSA's relationship with the academic community in matters of public cryptography;
>
> (e) what can and should be NSA's response (if any) to the public in matters of public cryptography.[80]

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

(U) ~~(FOUO)~~ [redacted] The board contained consultants from industry, academe, and government, in addition to its NSA representatives. Meeting throughout 1978, the Task Group focused on NSA's roles and responsibilities with respect to national security, national interest, and public cryptographies.

~~(C)~~ The Task Group, which issued its final report after Inman had already made his decision to seek additional legislation, confirmed that NSA should continue to assume full responsibility for National Security Cryptography.[81] There was almost no chance that the NSA would relinquish any part of what it considered its primary COMSEC mission. In addition, PD-24 clearly recognized that NSA was to be the sole executive agent for National Security Cryptography.

~~(S-CCO)~~ While the Task Group embraced PD-24 for National Security Cryptography, it took a different approach to National Interest Cryptography. PD-24 removed national interest cryptography responsibility from the NSA, eliminating NSA as the sole executive agent for all government cryptography. The Task Group accepted this fact but noted that "one can hypothesize a set of actions which would result in NSA again becoming the sole executive agent [of all government cryptography]."[82] This course of action required a transition step, which is exactly what the Task Group recommended. Specifically, the Task Group believed NSA's interim national interest policy should be

> To reserve to itself, with the approval of the President, the responsibility for approving the cryptographic techniques (algorithms, systems) and R&D efforts to be applied or suggested by other Federal agencies in carrying out their assigned National Interest or Public Cryptography responsibilities.[83]

~~(S-CCO)~~ The Task Group was cognizant of the political difficulties in regaining NSA's cryptographic monopoly of national interest cryptography. They believed that this option, however, would provide the opportunity to demonstrate NSA's concerns to Congress and the president. Eventually, the Task Group believed, PD-24 should be eliminated and NSA should again become sole executive agent for National Interest Cryptography.

~~(C)~~ While the Task Group saw the need for greater NSA involvement in National Interest Cryptography, it took a surprisingly limited approach to public cryptography policy. As a statement of policy, the Task group recommended that

> The Federal Government should assume no responsibility for Public Cryptography unless assigned by statute or executive order for specific cases.[85]

Like the earlier DDO/DDR position presented to Inman, the Task Group's position on public cryptography attempted to avoid any free speech issues by maintaining a complete hands-off approach to all nongovernment cryptography. The Task Group saw a need to balance legitimate academic research with NSA security concerns. Thus, NSA would take no action against nonfederally funded cryptographic research while simultaneously obtaining greater control over federally funded cryptographic research.

~~(S)~~ Overall, the NSASAB Task Group's recommendations reinforced NSA's desire to regain control over the field of cryptography. NSA general counsel Silver noted in response to the Task Group that "achieving a monopoly over approval of cryptographic techniques and R&D efforts for the Federal Government should be a high priority item for the Agency."[86] NSA saw PD-24 as a poor national policy and was beginning to lay the foundation for its reversal.

~~(S)~~ At the same time, the NSASAB Task Group's recommendations did not support Inman's prior policy decision to develop new legislation for the restriction of public cryptography. The Task Group paid serious attention to the concept of academic freedom, stressing that government funding of cryptographic research was necessary if one was to justify NSA intervention in public cryptography. However, DDO McFadden, who had earlier noted the limited danger of nongovernment-funded cryptographic research, had by this time come to the opposite conclusion that "the threat from [public cryptography], even if all other areas are constrained, is sufficiently great that NSA should seek legislative constraints."[87] General Counsel Silver suggested that the Task Group's recommendation be read as a hands-off to coercive or extralegal efforts, while not prohibiting NSA from seeking additional legal means to control public cryptography.[88] Clearly, the desire to control cryptography, be it national security, national interest, or public, was still present at NSA.

FURTHER JUSTIFICATION

~~(S)~~ While the NSASAB Task Group was preparing its report, Inman asked another group to provide further justifications to support additional restrictions on public cryptography. Inman had been attempting to sell Congress on the idea of new protections for cryptographic information. Constant meetings with Congress had convinced Inman that he needed specific examples to demonstrate the danger that unrestrained public cryptography placed on national security. In response to this, Inman formed an ad hoc committee consisting of the DDO, DDR, DDC, and DDT to examine the probable impact of unchecked public cryptography on the NSA's mission in the medium-range future. Inman believed that this ad hoc group's results would have "substantial importance in the efforts [NSA has] decided to undertake in the direction of strengthening governmental controls over the dissemination of cryptologic information."[89]

~~(TSC)~~ SIGINT concerns dominated the ad hoc committee's discussions.

~~(TSC)~~

~~(S)~~

~~(S)~~ The ad hoc committee saw a definite need for NSA action to prevent damage to the Agency's mission. They concluded unanimously that "it is virtually certain that some of the developments that can be seen in public cryptology will result in serious damage to the Agency's mission unless they are countered by actions in the interests of national security."[93] Like the NSASAB Task Group, the ad hoc committee stressed that NSA needed the authority to control all government activities involving cryptography. However, while the ad hoc committee focused on efforts sponsored by other government organizations, it also believed nongovernment research posed a threat "of similar technological magnitude."[94] The ad hoc committee recommended close monitoring of nongovernmental efforts, and it did not rule out the possibility of additional legislation at some future time. With this justification of the need for new controls on public cryptography, Inman continued his efforts to produce additional legislation.

CRYPTOLOGIC INFORMATION PROTECTION ACT OF 1979

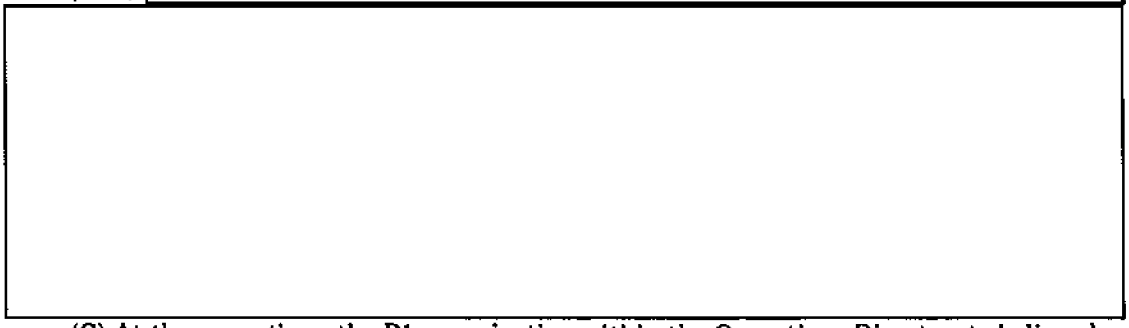
(U) ~~(EQUO)~~ In January 1979 General Counsel Silver distributed a draft version of the Cryptologic Information Protection Act of 1979. This statute would place significant restrictions on the dissemination of public cryptography information that might be harmful to national security. The Agency realized the political difficulty of obtaining such legislation, recognizing that "only the narrowest and most carefully drawn statute has any chance of success."[95]

(U) ~~(EQUO)~~ The draft statute created a new entity, the United States Cryptologic Board. It would consist of representatives from the secretary of defense, the secretary of commerce, the director of NSA, and three other members appointed by the president. This board would have the ability to restrict the dissemination of public cryptographic material for up to five years. Those who knowingly and willfully disseminated restricted cryptologic information could be sentenced to up to five years of prison and up to $10,000 in fines. The statute provided for review of board decisions and compensation for those whose materials were restricted.[96]

~~(C)~~ Reactions to the draft statute were mixed. Minor changes were suggested by DDC and ADPR, but both were in strong support of the statute. ADPL also favored the general premise of the statute but believed major efforts were necessary to make it constitutionally and politically palatable. On the other hand, DDR did not believe such legislation was necessary, and DDT saw the need to consolidate government cryptography before worrying about nongovernmental efforts.

(b) (1)
(b) (3)-P.L. 86-36

~~(TSC)~~



~~(C)~~ At the same time, the P1 organization within the Operations Directorate believed the draft statute required additional safeguards to protect cryptographic information. P1 added a section on War Powers, which would allow the president to suspend the review process during a war and consider as treason the dissemination of restricted cryptographic information. Furthermore, P1 expanded the financial penalties to include a provision allowing NSA to recover damages incurred by the dissemination of restricted data.[99] DDO eventually supported the P1 position, but it forwarded the G Group concerns to Silver.[100]

~~(C)~~ Given the level of disagreement with the draft statute, Inman decided that additional work needed to be done prior to actually proposing legislation to Congress. Inman tasked those involved in the review of the draft statute to examine two new questions. First, they were to consider the legislative approach and develop what they viewed as a "least damaging" version. Second, they were to consider other approaches short of legislation that would also protect the NSA mission with respect to public cryptography.[101]

~~(S-CCO)~~ Response to this request once again included a wide spectrum of opinions. R1 stressed that without government funding, public cryptography research would not require government control. As evidence, he stated that neither A nor G groups supported additional legislation.[102] Meanwhile, R5 noted recent public-key cryptography papers published openly and claimed that uncontrolled public cryptography research would clearly be "harmful to the national interests of this country."[103] In agreement, DDO argued that the larger goal of national security should supersede other concerns. DDO asserted that the damage of open public cryptography research had been demonstrated, and legislation was the only feasible means of dealing with this long-term problem.[104]

~~(FOUO)~~ The debate convinced Inman that additional protections were necessary to control the spread of public cryptography technology. As a practical matter, Inman realized that the chance of obtaining legislation that further restricted public cryptography was small. In order to increase the odds, NSA would need to improve its image and would need to convince Congress and the public that its national security interests were valid and reasonable. Given the significance of the public cryptography debate, Inman believed that the time had come for NSA to go public.

NSA SPEAKS OUT

(U) Traditionally, NSA directors did not involve themselves in public discussions of the Agency's missions. The adage that NSA implied "Never Say Anything" was applied to all working at the NSA. However, Inman saw the need to repair the damage that recent media exposure had caused. He felt that both Congress and the executive branch were basing their opinions of NSA operations on what they received from the media; thus it was essential to present NSA's side of the story to the media.

(U) Inman's first foray into the public arena was an interview in *Science* magazine in October 1978. He proceeded to discuss NSA's view on several of the recent public cryptography controversies. He outlined the bureaucratic problems that had occurred with patent secrecy orders and explained the changes NSA had made to its system. Inman stressed both his commitment to allowing openness when possible and restricting dissemination when necessary.[105]

(U) Inman's next public move was the January 1979 meeting of the Armed Forces Communications and Electronics Association (AFCEA). A speech, entitled "The NSA Perspective on Telecommunications Protection in the Public Sector," was prepared for Inman by the COMSEC office (S Group). The speech once again outlined several of the recent issues that had been highlighted in the press and provided NSA's viewpoint on each of them. The Senate's exoneration of NSA's role in the creation of DES, the Agency's uninvolvement with the Meyer letter to IEEE and NSA's resulting efforts to clarify ITAR, the reexamination of the NSA's secrecy patent rules, and the limited role NSA played in the granting of NSF public cryptography research funds were all mentioned as demonstrating NSA's openness to a reasonable level of dissemination of public cryptography information.[106]

(U) However, Inman stressed to this receptive crowd that NSA's national security concerns also needed to be considered in the public cryptography debate. He noted that

> The crux of the problem is that increased concern over telecommunications protection in the nongovernmental sector implies increased public knowledge of communications protective techniques. The principal 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.[107]

(U)(~~FOUO~~) Inman further argued that he believed present legislative recourses available to the Agency were insufficient to protect from this erosion of national security. He argued that the current safeguards needed to be strengthened, especially with respect to the export of cryptographic information and devices. While Inman did not mention the legislative effort currently under consideration at NSA, he did emphasize the characteristics that he believed any new legislation would need to possess. These features included granting a strong protection for basic scientific research, placing the burden of proof for restriction on the government, allowing judicial review of government decisions,

and providing compensation for those whose works were restricted.[108] While Inman did not mention NSA's current legislative draft by name, it is clear that his speech was geared to introducing NSA's new proposal to the public.

(U) ~~(FOUO)~~ Inman's decision to make public comments was not universally accepted within NSA. In situations where public involvement was possible, Inman generally received widely conflicting advice from his Key Components. Overall, Inman attempted to comment only in situations where a technical discussion of the field of cryptography was unlikely. As an example, Inman was given the chance to provide a review of the article "The DES Controversy Examined" by Hellman which would be appearing in the publication *SPECTRUM*. The review, if critical, could be published without attribution following the article. Upon seeking advice from NSA offices involved in the public cryptography debate, Inman was asked not to comment at all by D4 (policy staff), ADPL, and G03.[109] However R1, DDC, and the general counsel believed that a substantive rebuttal could be made that was more focused on policy.[110] Inman decided on this latter approach, citing both the Senate's DES hearings and his own AFCEA speech in the rebuttal.[111]

(U) ~~(FOUO)~~ Inman's goal was to convince both the public and the government that NSA could be reasonable in its approach to public cryptography. Inman attempted to counter the bad publicity NSA had received because of its relationship with public researchers and to initiate a dialogue to find the correct policy for public cryptography. By this time, Inman had come to distrust the NTIA's actions in this field, and he believed that much of the fear-mongering about devious NSA intentions were in fact being spread by individuals at the NTIA.[112] Inman's public initiatives were fairly successful. The new openness of NSA helped Congress rethink the need for NTIA and helped researchers accept the NSA's invitation for a dialogue.

AMERICAN COUNCIL ON EDUCATION

(U) In response to Inman's request for a dialogue with academics, the American Council on Education (ACE) initiated an effort to bring NSA representatives and academicians together to discuss the issue of public cryptography. The initial meeting in May 1979 concluded that a study group should be created to examine the national security and academic freedom questions raised by public cryptography. The goal of such a group would be to examine the current legislation and federal procedures with respect to the needs of NSA and academia.[113]

(U) Inman supported the creation of a study group involving academics to examine public cryptography policy. He proposed that the group be kept relatively small and that it consist of representatives from the professional societies most likely to be involved with public cryptography.[114] In terms of funding for such a group, Inman felt that direct funding of such a study by NSA would necessarily cast a shadow over any results obtained. Thus,

Inman recommended that ACE apply for National Science Foundation (NSF) funding for the group.[115] In January 1980 NSF agreed to fund the study group.

(U) ~~(FOUO)~~ The first order of business was to determine who would be a member of the study group. NSA would be represented by its general counsel, Daniel Schwartz, who had by this time taken over the position vacated by Daniel Silver. In addition, the NSA delegation would include technical observers, such as Richard Leibler, chief of R5. The other members would represent mathematical, computer science, and electrical engineering professional societies. Schwartz suggested that the committee be chaired by an academic legal expert, mentioning Ira Heyman, an official from the University of California, as a possible choice.[116] NSA wanted, however, to create a study group which would be viewed by academicians as independent. Davida, who remained antagonistic to NSA from his earlier patent secrecy experience, was chosen as a member representing the IEEE Computer Society. Likewise, Hellman was first involved as an observer and later involved as a member representing IEEE.

(U) The first meeting of the working group was held in March 1980. Werner Baum, who was chancellor at the University of Wisconsin-Milwaukee during the Davida secrecy patent episode, chaired the meeting. He noted from the outset that "it ought to be possible to do something to protect legitimate interests in classifying some things and protect free rights of research and associated property rights."[117] Davida, however, argued that any proposal to regulate research in public cryptography would be unworkable and doomed to failure.[118] The result of the meeting was an agreement by NSA to draft a statement of the issues which could be circulated for discussion. Given an agreement on the issues, the working group could then examine its alternatives.[119]

(U)~~(FOUO)~~ Schwartz summed up the point to be debated as follows:

> The principal issue is the extent to which concerns for the national security should in any way hinder or limit research, commercial development, or discussion in the non-governmental arena relating to telecommunications protection through means of cryptography.[120]

This statement of the issues document was circulated among several Agency seniors for their opinions. Most provided minor editorial changes to the paper, and DDPP also suggested providing the working group with a copy of Inman's AFCEA speech. However, some were adamantly opposed to both the statement and the working group effort. A5 asserted in no uncertain terms that "the worst thing NSA can do is to get into a debate with either individuals or groups supporting public cryptography."[121] Inman eventually supported Schwartz's statement, and it was distributed to the working group along with the text of Inman's AFCEA speech.

(U) The statement of issues was discussed at the second meeting of the working group in May 1980. Davida, still opposed to any form of government interference in public cryptography, argued that no problem currently existed and that national security concerns should center more on the economic necessity of strong public cryptography. Finally, a vote was taken on whether the working group should accept both that the current public cryptography situation could harm national security and thus that a system

of prior restraint of publication of articles was conceivable. The vote was 7-1 in favor, with Davida casting the lone dissent. The working group then created two subcommittees, one tasked with formulating procedures for prior review and the other preparing a document on the nature of the cryptography that was to be covered by the policy.[122]

(U) NSA was initially involved in the procedures subcommittee. Schwartz submitted the draft Cryptologic Information Protection Act of 1979 as a possible model for the restraint of public cryptography information. The subcommittee made several important changes to the draft proposal. First, the process would be voluntary with no penalty for those who did not submit their publications. Next, the information covered would be very narrowly defined, centering on application of cryptologic principles as opposed to more theoretical research. Also, the information would first be reviewed by a board of five members, the majority of whom were not NSA employees. Finally, NSA would not have the ability to restrain publication on its own but would need to receive a restraining order from a federal district court. While this was a significantly weaker document than the original draft, Inman saw it as his most realistic option for the restriction of public cryptography information.[123]

(U) The working group met again in October 1980 to discuss the results of the subcommittees. The draft from the procedures subcommittee was modified by the working group, expanding the advisory board from five members to seven and explicitly recognizing that the social concerns of public cryptography would be considered in any decision to restrain publication. In addition, the working group agreed only on the voluntary portion of the proposal, choosing to postpone any decision on additional NSA authority to obtain a restraining order until the voluntary system had operated for a two-year trial period. The group accepted this modified procedure, with the exception of Davida. The second subcommittee's description of what was to be covered also required additional work, and Leibler was assigned to assist in this effort. A final draft was scheduled to be completed by January.[124]

(U) Davida, unhappy with the current situation, soon employed the media to criticize the actions of the working group. *Science* published a critical review of the working group's proceedings, noting ominously possible NSA plans at the end of the two-year trial period. *Science* also asserted that NSA "confused" many of the participants, forcing them to "quickly concede" to the requests of the NSA. *Science* quoted one disgruntled anonymous member of the working group who had asked himself "what the hell do they [NSA] have up their sleeve?"[125] In addition, *Science* interviewed a working group observer Timothy Ingram, staff director for the House of Representatives Subcommittee on Government Information and Individual Rights, who observed:

> The questions are, what is the statutory authority for this censorship and what do these researchers get in exchange for what they are giving up? It's hard to see, other than a cage.[126]

(U) ~~(FOUO)~~ Several heated letters were exchanged between Davida and other members of the working group. Heyman and others resented Davida's implications that they were naively following NSA's orders. In November, Elwin Berlekamp, an IEEE representative

on the working group, felt it best if he resign from the group because of the perception that he was too closely attached to the NSA. Berlekamp was replaced by Hellman, who by this time believed that NSA's efforts were sincere and thus warranted academic cooperation.[127] Hellman, viewed by Davida and the media as a foe of the NSA, was able to moderate Davida's concerns. Thus, the final draft was completed and circulated for comment.

~~(C)~~ Given NSA's initial proposal, the procedure adopted by the ACE working group was clearly weak in the protection provided to NSA. No additional power to restrict the dissemination of public cryptography material was provided, and the case for academic freedom was clearly cited in the resulting proposal. Most organizations within the Operations Directorate, including G, A5, and P1, saw this document as a wholesale retreat from NSA's previous goals of strong new dissemination restrictions.[128] Others, such as DDC Howard Rosenblum, were satisfied that the working group attempted to balance the NSA and academic viewpoints with an amicable resolution.[129]

(U) ~~(FOUO)~~ The final policy was publicly distributed to the professional societies and was printed in journals such as *Cryptologia*. The NSA accepted these recommendations in May 1981. While the restrictions provided were weak, participation was fair. Davida himself submitted papers through the review process, and *Cryptologia* continues to submit each of its articles for NSA review.[130] Wounds inflicted by the acrimonious DES debate between NSA and public researchers were slowly beginning to heal.

OCREAE

(U) NSA was also pursuing another means of involving itself with academe. Earlier problems between NSA and the National Science Foundation over NSF's funding of public cryptography research had changed significantly. In a September 1978 meeting with Inman, Richard Atkinson, director of the NSF, had suggested that if NSA were to sponsor its own unclassified research program then perhaps NSF could reduce its funding in the field of public cryptography. Atkinson further offered Inman NSF support in establishing such a program.[131] Inman saw this as an opportunity to further bridge the gap between NSA and academe and enhance NSA's visibility in the technical community, and he replied to Atkinson that the offer was "most attractive."[132]

(U) ~~(FOUO)~~ Inman also saw NSF's offer as an important tool in asserting NSA's authority with respect to NTIA. By taking an aggressive step in funding domestic public cryptography research, NSA hoped to prevent NTIA from becoming more involved in the field. While an NTIA/NSA interface was discussed for this new research grant program, it was clear that NSA would play the dominant role in funding decisions.[133]

(U) Legal problems involving NSA's authority to issue research grants slowed progress on the program, but with support from William Perry, under secretary of defense for research and engineering, Inman was eventually able to establish OCREAE in 1980. According to the OCREAE brochure distributed to universities:

> The objective of the NSA OCREAE Program is to nurture basic research that may lead to advances in cryptologic techniques and contribute to current knowledge. Support shall be made available for basic research in mathematical disciplines and computational science related to cryptography.[134]

HOUSE COMMITTEE ON GOVERNMENT OPERATIONS

(U) NSA's attempts to reach out to public researchers were viewed suspiciously by some members of the House Committee on Government Operations. The Subcommittee on Government Information and Individual Rights was concerned with NSA's efforts to classify or restrict private ideas. In February 1980 the subcommittee invited two of NSA's staunchest critics, George Davida and David Kahn, to join Inman in a panel discussion of NSA's public cryptography policy. The result of the subcommittee's hearings was a highly critical report of NSA's public cryptography initiatives. Specifically, the subcommittee detailed two separate areas in which it believed NSA's efforts posed "enormous questions of constitutional validity."[135]

(U) First, the subcommittee examined NSA's attempt to establish a voluntary prior restraint on the publication of public cryptography information. While the subcommittee viewed NSA's dialogue with the academic community as a "welcome development," it expressed its reservations with the very concept of any form of prior restraint on private ideas. It noted that First and Fifth Amendment rights needed to be considered in any such proposal, and it criticized NSA for not providing the academics in the ACE working group with a copy of the Justice Department's view on the unconstitutionality of ITAR.[136]

(U) Inman attempted to counter the subcommittee criticism, noting that he had "not lightly accepted the position that unrestricted nongovernmental cryptologic activity poses a threat to the national security."[137] However, both Kahn and Davida argued otherwise. Kahn stated that any attempt to "police ideas . . . would be very deleterious and would harm the nation a great deal more than it would help it."[138] Davida agreed with this sentiment and further stressed that even if such restrictions were desired, they would be impossible to implement. While Inman reiterated the voluntary nature of the restraint, Kahn and Davida warned of its ominous implications. Both Kahn and Davida stated explicitly that there should be no limitations placed on the study of cryptography, while Inman argued that some regulations were necessary. In the end, the subcommittee's report issued its recommendation that NSA end its policy of "the less published in public cryptography, the better."[139]

(U) Next, the subcommittee explored NSA's relationship with the NSF. The subcommittee noted that NSA was clearly attempting to assume responsibility from the NSF for unclassified public cryptography research. As evidence, the subcommittee cited claims NSA had made to NSF that NSF funding of public cryptology was illegal and claims by NSA that it was the only agency with the expertise to evaluate public cryptography funding. The subcommittee pointedly remarked that it had "not tried to determine whether the National Security Agency tendency to advance exaggerated claims

of authority in its dealings with the National Science Foundation stems from conscious policy or the actions of individual NSA employees."[140]

(U) The subcommittee's main concern was that NSA's OCREAE program would allow the NSF to reduce or eliminate its funding of public cryptography research. It was noted that the Senate Intelligence Committee's hearings of 1978 had already recognized that NSF needed to consider the national security implications of its funding, a proposition that the NSF had earlier rejected. Now, it appeared that the NSA was attempting to completely eliminate NSF involvement in the funding process. The subcommittee argued that while NSA could fund its own public cryptography research, it should not affect NSF's efforts in the field. Moreover, the subcommittee recommended that NSF eliminate NSA's involvement in NSF's grant review process. They categorically refused to allow NSA to use national security considerations as a reason to review NSF grants.[141]

(U) Clearly, Inman was not pleased with the final report of the House subcommittee. The recommendations by the subcommittee sought to marginalize NSA's involvement with public cryptography policy. NSA's national security arguments were strongly rebuked as the subcommittee stressed the need for a strong nongovernmental program of public cryptography research. Inman's request that the subcommittee consult with either the House or Senate Intelligence Committees, two committees that had access to classified information which would further support Inman's position, was ignored.[142]

(U) (~~FOUO~~) In response to the report, Inman voiced his complaints to others in Congress that he believed would be more sympathetic. Deciding against involving either the secretary of defense or the director of Central Intelligence, Inman went directly to Congressman Edward Boland, who chaired the House Intelligence Committee.[143] Inman informed Boland that the House Government Operations report suggested actions that Inman felt were "contrary to the national interest."[143] Noting that he believed Boland's committee to be "uniquely qualified" to evaluate NSA's concerns, Inman suggested that Boland undertake a review of the report.

(U) (~~FOUO~~) Eventually, Boland decided that no additional review was necessary. The political landscape had changed since the time the subcommittee had first examined the NSA and public cryptography. Congressman L. Richardson Preyer (D-NC), who chaired the subcommittee and led the attack on NSA, had been defeated in his bid for reelection. Boland did inform Congressman Jack Brooks, chairman of the Government Operations Committee, that any future discussion of public cryptography should be coordinated with the Intelligence Committee.[145] More importantly, this episode demonstrated to Boland the confusion that still existed with public cryptography policy in general.

NATIONAL POLICY

(U) In November 1979, Dr. Frank Press, the director of the Office of Science and Technology Policy, instructed the secretary of commerce and the secretary of defense to jointly develop a policy on public cryptography in response to PD-24. Once again, an effort

was being made to sort out the direction that various government institutions would take with respect to public cryptography. No progress was made by Commerce and Defense working groups, and by September 1980 they were tasked with submitting separate proposals detailing their positions on the various public cryptography issues.[146]

(U) The Defense Department position was largely drafted by NSA. First, the DoD position asserted that NSA should have the ability to review, for impact on national security, all government funding of public cryptography. This would include any research supported by NSF or NTIA. This goal had been one of the first considered by NSA as a way of dealing with increased research in public cryptography. Next, the DoD position noted that both secrecy patents and ITAR were useful, justifiable constraints that should be maintained. It stressed the applicability of these policies to high-grade cryptographic equipment, while underscoring the need for strong safeguards to prevent the improper use of these options. In addition, the DoD position encouraged "the transfer of the Federal government's expertise and technology in cryptography to the private sector, within national security concerns."[147] To this end, the federal government would certify public cryptography standards. Specifically, the DoD position recognized the need to continue validating manufacturers' implementations of DES.[148]

~~(C)~~ The most contentious portion of the DoD proposal involved domestic publication of public cryptography research. NSA was still involved in its discussions with the ACE working group and hoped to secure some form of prior review over public cryptography papers. However, the original DoD proposal stated that no special controls would be placed on domestic publication of public cryptography data. Inman personally contacted Ronald Stivers, the acting deputy under secretary of defense, who was coordinating the DoD position. Inman stressed his strenuous opposition to this policy against special controls, noting that academe seemed willing to accept some form of voluntary restraint.[149] NSA's position was finally accepted and forwarded as a DoD policy recommendation to Press.[150]

~~(C)~~ Overall, the DoD recommendations represented a fairly aggressive attempt by NSA to assert national security, as represented by SIGINT and COMSEC interests, as the primary motivating factor in the public cryptography debate. Following some of the initial recommendations of the 1978 Task Group on Public Cryptography, NSA was taking a fairly hands-off approach to academics while simultaneously expanding its authority over government public cryptography efforts. By this time, NSF had stated that it would allow NSA to review proposals for technical merit and classify results when necessary. Thus, the DoD proposal sought to make permanent some of the gains that NSA had obtained under Inman.

(U) The position paper prepared by NTIA for the Commerce Department was somewhat different. While it recognized some national security concerns, it also stressed the need to "preserve a climate of freedom by minimizing government interference in the private sector."[151] Specifically, the NTIA argued that national public cryptography policy required a significant increase in government funding of public cryptography research, coupled with reducing or eliminating many of the restrictions found in ITAR and secrecy

patents. With regard to NSA's efforts to obtain voluntary prior restraint on public cryptography publications, the NTIA noted "efforts to discourage technological progress through voluntary restraints are likely to be futile and cause contention."[152] In general, NTIA believed that NSA's interests in public cryptography were often overstated and needed to be balanced with other national interests.

(U) The DoD and Commerce positions were forwarded to Press, but again the 1980 presidential election had started to change the policy landscape. The NTIA White Paper was provided to Congressman Boland, chairman of the House Intelligence Committee, who by this time had come to support the NSA position on public cryptography. The release of the NTIA proposal coincided with the release of the Committee on Government Operations report, and both indicated to Boland the difficulties NSA was facing with respect to public cryptography. As a result, Boland informed the now President Ronald 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. cryptologic 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. . . .[153]

~~(C)~~ A major goal of the 1978 Task Group on Public Cryptography, the repeal of PD-24, now had congressional support. Eventually, PD-24 would indeed be eliminated and replaced with NSC-145, which once again vested government cryptology efforts with the NSA. However, this too would be repealed as the debate over NSA's role in public cryptography continued.

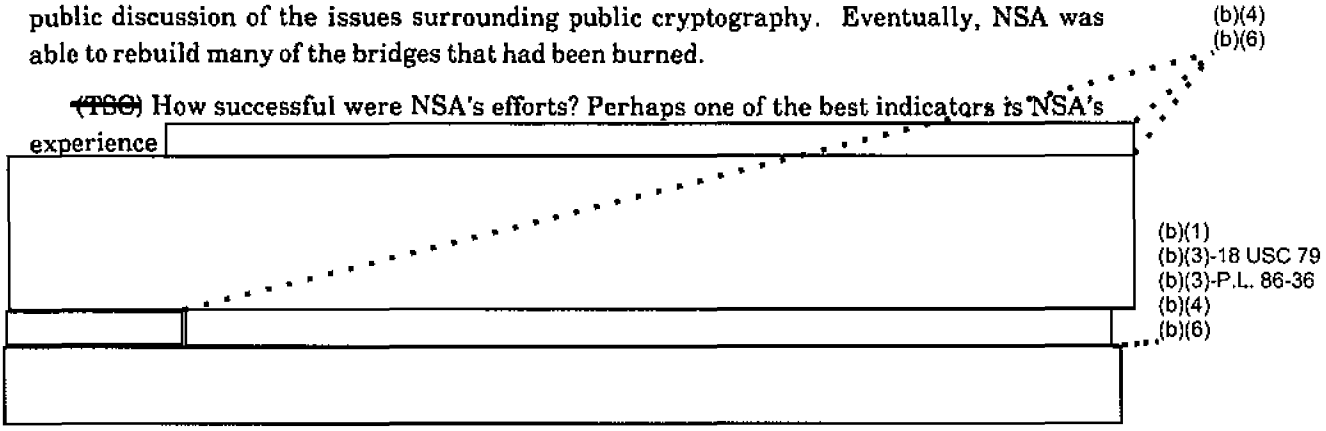
CONCLUSION

~~(C)~~ Prior to DES, NSA had achieved an almost exclusive hold on U.S. cryptographic efforts. Industry and academe had little use for the esoteric art of cryptography, and NSA was able to exert significant influence over the small pool of individuals who did work in the field. With DES came change, and NSA no longer had absolute control over cryptology. The world had changed, and NSA policy needed to change with it.

(U) Recognizing that "the genie was out of the bottle" with public cryptography, NSA attempted to put itself in the position where it could at least maintain its control over

government efforts in cryptology. In doing so, several embarrassing public missteps were made which earned the NSA the mistrust of Congress, academe, and the public. In trying to fight this perception of NSA heavy-handedness, Inman made the decision to engage in a public discussion of the issues surrounding public cryptography. Eventually, NSA was able to rebuild many of the bridges that had been burned.

~~(TSC)~~ How successful were NSA's efforts? Perhaps one of the best indicators is NSA's experience



(U) While public cryptography problems continued to grow after Inman left NSA, the Inman era was useful in highlighting both the issues and the fundamental concerns of NSA in the area of public cryptography. Thus, while many of NSA's policy objectives went unfulfilled, the Inman era produced a foundation of increased academic and public trust which offered the hope that a rational discussion of NSA's role in public cryptography could be obtained.

Notes

1. Report of the Task Group on "Public Cryptography," National Security Agency Scientific Advisory Board, October 1978 ~~(S-CCO)~~. Hereafter, Task Group on "Public Cryptography."

2. Ibid.

3. NSA Involvement in the Development of the Data Encryption Standard, 1978 Senate Intelligence Committee Report ~~(S-CCO)~~.

4. Task Group on "Public Cryptography."

5. Paul Kinnucan, "Data Encryption Gurus: Tuchman and Meyer," *Mini-Micro Systems*, Volume II, Number 9, October 1978 (U).

6. Task Group on "Public Cryptography."

7. NSA Involvement in the Development of the Data Encryption Standard, 1978 Senate Intelligence Committee Report ~~(S-CCO)~~.

8. "History of U.S. Communications Security," The David G. Boak Lectures, Volume II, July 1981 ~~(S-CCO)~~.

9. Task Group on "Public Cryptography."

10. NSA Interview, Richard Proto, 3 July 1995, by [redacted] 32-95, Center for Cryptologic History ~~(TSC)~~; also Proto, Richard, Memorandum on Public Cryptography, 7 May 1980 ~~(S)~~.

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

11. Task Group on "Public Cryptography."

12. NSA Involvement in the Development of the Data Encryption Standard, 1978 Senate Intelligence Committee Report ~~(S-CCO)~~.

13. Task Group on "Public Cryptography."

14. Gina Bari Kolata. "Computer Encryption and the National Security Agency Connection," *Science*, Volume 197, 29 July 1977 (U).

15. David Kahn, "Tapping Computers," *The New York Times*, 3 April 1976 (U).

16. Ibid.

17. NSA Involvement in the Development of the Data Encryption Standard, 1978 Senate Intelligence Committee Report ~~(S-CCO)~~.

18. Robert Morris, N. J. A. Sloane, and A. D. Wyner. "Assessment of the National Bureau of Standards Proposed Federal Data Encryption Standard," *Cryptologia*, Volume 1, Number 3, July 1977 (U).

19. Minutes of the Board of Governors Meeting, IEEE Information Theory Group Newsletter, June 1977 (U).

20. Task Group on "Public Cryptography."

21. Report of the Ad Hoc Group on "Public Cryptography II," National Security Agency Advisory Board, July 1983 ~~(TSC)~~.

22. Chronology of contacts with NSF, W.P. Sullivan, 27 October 1977 ~~(S)~~.

23. Memorandum to Dr. John Pasta, NSF, 11 May 1977 (U).

24. James Bamford. *The Puzzle Palace*. Houghton Miffin Company, 1982(U).

25 [redacted] Memorandum for the Record, 6 September 1977 ~~(S-CCO)~~.

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

26. Ibid.

27 [redacted] Memorandum for the Record, 19 September 1977 ~~(S-CCO)~~.

28 [redacted] Memorandum to Inman, 19 October 1977 ~~(S-CCO)~~.

29. B. R. Inman,. Memorandum to RADM Robert Geiger, USN, Chief of Naval Research, 21 October 1977 ~~(C)~~.

30. Joe A. Meyer. "On the Release of Cryptologic Techniques," 3 May 1977 ~~(S-CCO)~~.

31. Joe A. Meyer. "On the Release of Cryptologic Techniques," 3 May 1977. ~~(S-CCO)~~. Norman Boardman, Memorandum on Controlling Cryptologic Publication, 5 May 1977 (U).

32. Joe A. Meyer. Letter to E. K. Gannet, IEEE Staff Secretary, Publications Board, 7 July 1977 (U).

33., E.K. Gannet Letter to Joe A. Meyer, 20 July 1977 (U).

34. NSA Involvement in the Development of the Data Encryption Standard, 1978 Senate Intelligence Committee Report ~~(S-CCO)~~.

35. W. P. Sullivan "Memorandum for the Record on Meeting with Staff Members of the Senate Select Committee on Intelligence Regarding Public Cryptography," 3 November 1977 ~~(S)~~.

36. B. R. Inman, Memorandum to Stan Taylor, Staff Member, Senate Select Committee on Intelligence, 14 December 1977. ~~(S)~~ B. R Inman, Memorandum to Don Edwards, Chairman, House Subcommittee on Civil and Constitutional Rights, 16 November 1977 (U).

37. Malcolm W. Browne, "Scientists Accuse Security Agency of Harassment Over Code Studies," *The New York Times*, 19 October 1977 (U).

38. NSA Involvement in the Development of the Data Encryption Standard, 1978 Senate Intelligence Committee Report (~~S-CCO~~).

39. Ibid.

40. Ibid.

41. Bruce Schneier, *Applied Cryptography*. John Wiley & Sons, Inc. 1994 (U).

42. Richard Proto, Chief R, "INFOSEC Posture and Threat," Kryptos/CMI talk given in Friedman Auditorium, 19 Jan 96 (U).

43. NSA Involvement in the Development of the Data Encryption Standard, 1978 Senate Intelligence Committee Report (~~S-CCO~~)

44. Jack Magarrell, "Senate Probe Finds Security Agency Didn't Harass Computer Scientists," *The Chronicle of Higher Education*, 17 April 1978, (U), Deborah Shapley, "Security Agency's Role in DES Confirmed," *Science*, 28 April 1978 (U).

45. Roy Banner, NSA General Counsel, Memorandum to Deanne Siemer, General Counsel, Department of Defense, 15 November 1977 (U).

46. Roy Banner, NSA General Counsel, Memorandum to John Harmon, Assistant Attorney General, Department of Justice, November 1977 (U).

47. John Harmon, Assistant Attorney General, Department of Justice, Memorandum to Frank Press, Science Advisor to the President, on the Constitutionality Under the First Amendment of ITAR Restrictions on Public Cryptography, 11 May 1978 (U).

48. Ibid.

49. Daniel Silver, NSA General Counsel, Memorandum on the Legal Status of Controls on the Dissemination of Non-Governmental Cryptologic Information, 26 June 1978 (U).

50. Ibid.

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

51. James Michel. Memorandum to John Harmon, Assistant Attorney General, Department of Justice, 6 July 1978 (U).

52. Ibid.

53. Daniel Silver, NSA General Counsel, Memorandum to Colonel Wayne Kay, Senior Policy Analyst, Office of Science and Technology Policy, 2 November 1978 (U).

54. Paul Brady, NSA Acting General Counsel, Memorandum t[redacted] Q4, on the Application of the Arms Export Control Act and the International Traffic and Arms Regulation, 18 September 1981 (~~FOUO~~).

55. Eugene Yeates, NSA Office of Legislative Affairs, Chronology of Professor George I. Davida's Patent Application (~~S-CCO~~).

56. Ibid.

57. Deborah Shapley, "Intelligence Agency Chief Seeks 'Dialogue' with Academics," *Science*, 27 October 1978 (U).

58. Howard Rosenblum, DDC, Memorandum to NSA General Counsel on Secure Communication System, 19 June 1978 (~~S~~).

59. Deborah Shapley, "Intelligence Agency Chief Seeks 'Dialogue' with Academics," *Science*, 27 October 1978 (U).

60. Daniel Silver, NSA General Counsel, Letter to Aldo J. Test regarding U.S. Patent Application #843800 Filed 20 October 1977 by Carl Nicolai, et al., 6 October 1978 (U).

61. Telecommunications Protection Policy, Presidential Directive 24, 16 November 1977 (~~S~~).

62. Paul Bortz, Deputy Assistant Secretary-designate NTIA, and Vice Admiral B. R Inman, NSA, Memorandum to Dr. Frank Press, Director Office of Science and Technology Policy, 9 November 1978 (~~S~~).

63. Ibid.

(b)(1)
(b)(3)-P.L. 86-36

64. [redacted] Memorandum for the Record on Conference to Discuss the Impact of Public Cryptography on NSA [redacted]

65. Ibid.

66. Ibid.

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

67. Ibid.

68. William Gerhard, Memorandum for the Record, 7 October 1977 (~~S~~).

69. [redacted] Chief S6, Memorandum to DDC on Cryptologic Research in Academe, 11 May 1978. (~~S~~) Philip Dibben, Chief A5, Memorandum to DDO on NSA Policy on Public Cryptologic Research, 30 May 1978 (~~S-CCO~~).

70. [redacted] Memorandum to W. Lutwiniak, Chief P1, on GC memo on Public Cryptography, 15 August 1978 (~~S-CCO~~).

71. Daniel Silver, NSA General Counsel, Options Paper on NSA Policy on Public Cryptology, 10 July 1978 (~~C~~).

72. John R. Harney, ADPL, Options Paper on NSA Policy on Public Cryptology, 21 July 1978 (~~C~~).

73. Howard Rosenblum, DDC, Options Paper on NSA Policy on Public Cryptography, 24 July 1978 (~~C~~).

74. Rear Admiral E. S. Ince, USN, DDT, Options Paper on NSA Policy on Public Cryptology, 27 July 1978 (~~C~~).

75. [redacted] DDR, Options Paper on NSA Policy on Public Cryptology, 24 July 1978 (~~C~~).

76. Major General George McFadden, U.S. Army, DDO, NSA Policy on Public Cryptology, 25 July 1978 (~~C~~).

77. Daniel Silver, NSA General Counsel, Policy Options on Public Cryptology, 9 August 1978 (~~C~~).

78. Daniel Silver, NSA General Counsel, Policy Options on Public Cryptology, 27 July 1978 (~~C~~).

79. Daniel Silver, NSA General Counsel, Public Cryptology, 23 August 1978 (~~C~~).

80. Task Group on "Public Cryptography."

81. Ibid.

82. Ibid.

83. Ibid.

84. Ibid.

85. Ibid.

86. Daniel Silver, NSA General Counsel, Memorandum on the NSASAB Report on Public Cryptography, 24 November 1978 (~~S~~).

87. Major General George McFadden, U.S. Army, DDO, Memorandum on the NSASAB Report on Public Cryptography, 27 November 1978 (~~S~~).

88. Daniel Silver, NSA General Counsel, Memorandum on the NSASAB Report on Public Cryptography, 24 November 1978 (~~S~~).

89. Vice Admiral B. R. Inman, USN, DIRNSA, Memorandum on the Assessment of Future Developments in Public Cryptography, 15 September 1978 (~~S~~).

90. Major General George McFadden, U.S. Army, DDO, Memorandum of Ad Hoc Committee to Assess Future Developments in Public Cryptology, 30 October 1978 (~~TSC~~).

91. Ibid.

92. Ibid.

93. Ibid.

94. Ibid.

95. Daniel Silver, NSA General Counsel, Memorandum on the Draft Statute Imposing Controls on Dissemination of Nongovernmentally Developed Cryptologic Information, 8 January 1979 (~~FOUO~~).

96. Ibid.

97. Peter A. Jenks, Deputy Chief of G, Comments on Draft Statute Imposing Controls on Dissemination of Nongovernmentally Developed Cryptologic Information, 17 January 1979 (~~TS~~).

98. Ibid.

99. William Lutwiniak, Chief of P1, Memorandum on the Draft Statute on Control of Cryptologic Information, 17 January 1979 (~~TS~~).

100. Major General George McFadden, U.S. Army, DDO, Memorandum on the Draft Statute Imposing Controls on Dissemination of Nongovernmentally Developed Cryptologic Information, 23 January 1979 (~~FOUO~~).

101. Daniel Silver, NSA General Counsel, Memorandum on the Draft Statute Imposing Controls on Dissemination of Non-Governmentally Developed Cryptographic Information, 27 February 1979 (~~TS~~).

102. [redacted] Chief of R1, Memorandum on Alternatives to Legislative Controls for Public Cryptography, 27 February 1979 (~~TS~~). (b) (3)-P.L. 86-36

103. [redacted] Chief of R51, Memorandum on Public Cryptography; 16 March 1979 (~~TSC~~).

104. [redacted] Technical Coordinator for DDO, Memorandum on Public Cryptography, 23 February 1979 (~~TSC~~).

105. Deborah Shapley, "Intelligence Agency Chief Seeks 'Dialogue' with Academics," *Science*, 28 October 1978 (U).

106. Speech by B. R. Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector," January 1979 AFCEA Symposium. (b) (3)-P.L. 86-36

107. Ibid.

108. Ibid.

109 [redacted] D4, Memorandum on IEEE Article "DES Controversy Examined," 24 April 1979 (~~S~~).

110. Ibid. Daniel Silver, NSA General Counsel, Note for the Director, 25 April 1979 (~~FOUO~~).

111. Vice Admiral B. R. Inman, USN, DIRNSA, Letter to Edward A. Torrerro, Senior Associate Editor *SPECTRUM*, 27 April 1979 (~~FOUO~~).

112. Interview of Admiral B. R. Inman by George Jelens, 16 December 1982 (U).

113. J.W.Peltason, President, American Council on Education, Draft of Letter to Executive Directors of Organizations Asked to Send a Representative to the Study Group, 23 July 1979 (U).

114. Vice Admiral B .R. Inman, USN, DIRNSA, Memorandum to Dr. J. W. Peltason, President, American Council on Education, 8 June 1979 (U).

115. Vice Admiral B. R. Inman, USN, DIRNSA, Memorandum to Dr. J. W. Peltason, President, American Council on Education, 15 November 1979 (U).

116. Daniel Silver, NSA General Counsel, Memorandum on the Follow-up on American Council of Education Meeting, 25 May 1979 (~~FOUO~~).

117. Daniel Schwartz, NSA General Counsel, Memorandum on the Meeting of the Public Cryptography Study Group, 8 April 1980 (~~FOUO~~).

118. Ibid.

119. Ibid.

120. Daniel Schwartz, NSA General Counsel, Memorandum on Public Cryptography, 21 April 1980 (U).

121. [redacted] Chief A5, Memorandum on Public Cryptography, 29 April 1980 (~~S~~).

122. Daniel Schwartz, NSA General Counsel, Memorandum on ACE Study Group on Public Cryptography, 3 June 1980 (~~FOUO~~).

123. Daniel Schwartz, NSA General Counsel, Memorandum on Public Cryptography Study Group, 4 August 1980 (~~FOUO~~).

124. Daniel Schwartz, NSA General Counsel, Memorandum on Public Cryptography Study Group, 9 October 1980 (~~FOUO~~).

125. Gina Bari Kolata, "Study Group Agrees to Voluntary Restraints," *Science*, Volume 210, 31 October 1980. (U)

126. Ibid.

127. Richard Severo, "Researchers to Permit Pre-publication Review by U.S.," *The New York Times*, 1 November 1980 (U).

128. William Lutwiniak, Chief P1, Memorandum on Sections I, II, and III of ACE Study Group Report, 18 December 1980. (~~FOUO~~) [redacted] Technical Director G, Memorandum on Sections I, II, and III of ACE Study Report, 23 December 1980 (~~FOUO~~). (b) (3)-P.L. 86-3

129. Howard Rosenblum, DDC, Memorandum on ACE Study Group Report, 22 December 1980 (~~FOUO~~).

130. Mike Levin, NSA Oral History Interview, 14 January 1987, by [redacted] OH-02-87 (~~S~~).

131. Richard Atkinson, Director, National Science Foundation, Letter to Vice Admiral B.R. Inman, 7 September 1978 (U).

132., Vice Admiral B. R. Inman, USN, DIRNSA, Letter to Richard Atkinson, Director, National Science Foundation, 21 September 1978 (U).

133. David Boak, Memorandum for the Record on NSF Proposal, 21 September 1978 (~~C~~).

134. "Grants and Cooperative Agreements for Research in Cryptology," NSA Brochure, August 1981 (U).

135. "The Classification of Private Ideas," The U.S. House of Representatives Committee on Government Operations, House Report 96-1540, December 1980 (U).

136. Ibid.

137. Ibid.

138. Ibid.

139. Ibid.

140. Ibid.

141. Ibid.

142. Ibid.

143. Daniel Schwartz, NSA General Counsel, Memorandum to DIRNSA on Letter to HPSCI Chairman Boland re Public Cryptography, 15 January 1981 ~~(POUO)~~.

144., Vice Admiral B.R. Inman, USN, DIRNSA, Letter to The Honorable Edward Boland, Chairman, Permanent Select Committee on Intelligence, U.S. House of Representatives, 16 January 1981 (U).

145. Congressman Edward Boland, Letter to The Honorable Jack Brooks, Chairman, Committee on Government Operations, U.S. House of Representatives, 3 February 1981 (U).

146. Henry Geller, Assistant Secretary for Communications and Information, Letter to Dr. Frank Press, Director, Office of Science and Technology Policy, 12 December 1980 (U).

147. Draft of DoD Recommendations on National Policy on Public Cryptography, September 1980 (U).

148. Ibid.

149. Vice Admiral B.R. Inman, USN, DIRNSA, Memorandum to Acting Deputy Under Secretary of Defense, 15 December 1980 (U).

150. Ronald Stivers, Acting Deputy Under Secretary of Defense, Memorandum to DIRNSA, 23 January 1980 (U).

151. NTIA White Paper on Analysis of National Policy Options for Cryptography, 29 October 1980 (U).

152. Ibid.

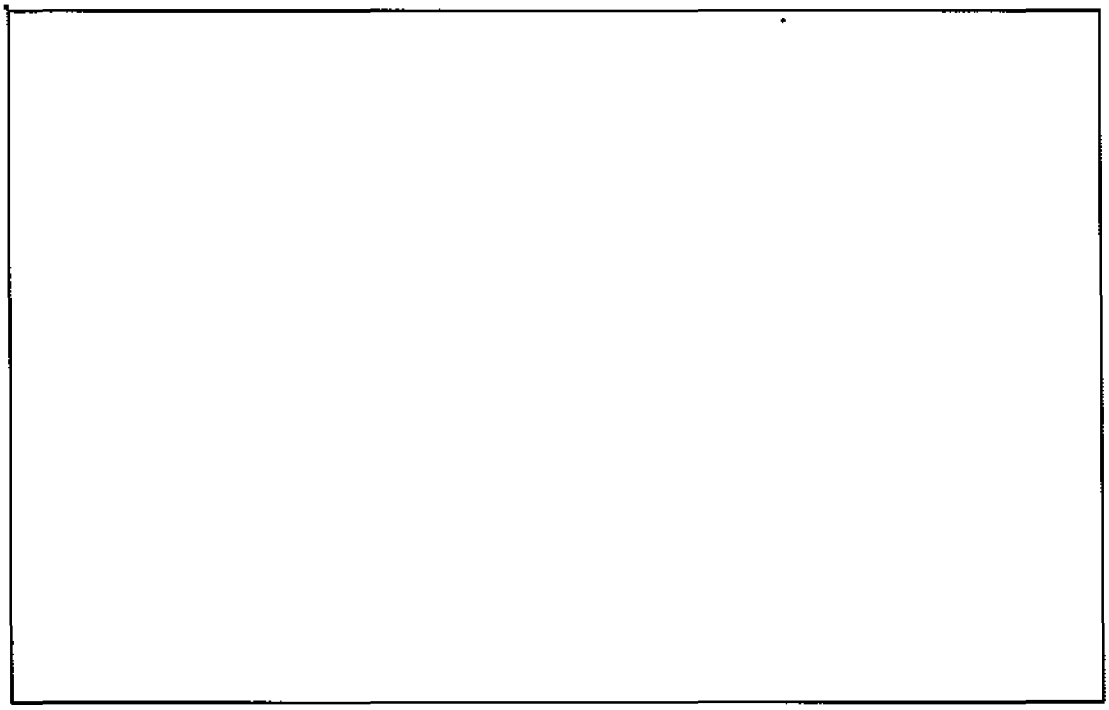
(b)(6)

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

154. [redacted] Memorandum for the Record of Meeting with [redacted] 9 May 1983 (U).

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

(b)(3)-P.L. 86-36
(b)(6)



Derived from: NSA/CSSM 123-2,
Dated 3 September 1991
Declassify On: Source Marked "OADR"
Date of source: 3 Sep 91