



OFFICE OF THE ASSISTANT TO THE SECRETARY OF DEFENSE
1400 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1400

19 MAY 1995

Ref: 95-F-0691



PUBLIC AFFAIRS

Mr. David A. Banisar
Electronic Privacy Information Center
666 Pennsylvania Avenue, SE, Suite 301
Washington, DC 20003

Dear Mr. Banisar:

This letter responds to your March 24, 1995, Freedom of Information Act (FOIA) request which was received in this Directorate March 27, 1995.

The enclosed documents are provided as responsive to your request.

There are no chargeable costs for processing your FOIA request in this instance.

Sincerely,

A. H. Passarella
Director
Freedom of Information
and Security Review

Enclosures:
As stated

#753

OFFICE OF THE DEPUTY SECRETARY OF DEFENSE

The Military Assistant

31 August 1994

MEMO FOR: MR. KEITH HALL, DASD/I (C3I)

Subject: Invite from NRC/NAS 7Oct94

Mr. Deutch's comment on the attached Invitation:

"Regret: JMD - Give to Keith Hall"

Very respectfully,



Pat Kane

Colonel, USA

Military Assistant to the

Deputy Secretary of Defense

Attachments

OSD 17592

SUSPENSE: _____

17592

NATIONAL RESEARCH COUNCIL/NATIONAL ACADEMY OF SCIENCES
COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD
2101 CONSTITUTION AVE., N.W., WASHINGTON, D.C. 20418
TELEPHONE: (202) 334-2605 FAX: (202) 334-2318

DATE: August 29, 1994 NUMBER OF PAGES INCLUDING THIS SHEET: 2

TO: John Deutch c/o Lynn Cline 703-697-9080 FROM: Herb Lin (202-334-3191 voice)

Professor Deutch:

As you may know by now, the NRC's committee to study national cryptography policy has been formed (and a list of the committee attached). The first meeting of the committee will be in October, and since you had expressed an interest in meeting with the committee to provide DOD perspectives on the subject, I am writing to solicit your participation at this meeting. In particular, we would like you to meet with the committee on Friday, October 7, some time in the morning, probably around 10:30 AM for about an hour (including discussion with the committee), at the Georgetown facility of the NRC. You should also know that we are trying to arrange briefings from other agencies (e.g., State and Justice), as well as from the intelligence community.

Your participation at this briefing would be enormously helpful to the committee.

Thanks in advance.



Herb Lin
Study Director and Senior Staff Officer

RK 29

X
//
||

COMMITTEE TO STUDY NATIONAL CRYPTOGRAPHY POLICY

(Biographies are being updated)

Kenneth Dam, committee chair, was Deputy Secretary of State (1982-1985) and is currently the Max Pam Professor of American and Foreign Law at the University of Chicago Law School.

General W. Y. Smith (ret.), committee vice-chair, is President Emeritus of the Institute for Defense Analyses, and has also served in a number of military posts including Deputy Commander in Chief of the U.S. European Command in Germany.

Lee Bollinger is Provost of Dartmouth College and a constitutional scholar.

Ann Caracristi, retired, was Deputy Director of the National Security Agency (1980-1982)

Benjamin Civiletti was U.S. Attorney General (1979-1981), and is currently in private practice with the law firm Venable, Baerjer, Howard and Civiletti.

Colin Crook is Senior Technology Officer for Citicorp

Samuel Fuller is Vice President of Corporate Research at Digital Equipment Corporation.

Leslie Gelb is President of the Council on Foreign Relations. He has also served as an Assistant Secretary of State for Politico-Military Affairs (1977-1980).

Ronald Graham is professor of mathematics at Rutgers University and Adjunct Director of Information Sciences at AT&T Bell Labs.

Martin Hellman is professor of Electrical Engineering at Stanford University. Dr. Hellman was one of the inventors of public key encryption.

Julius Katz is President of Hills & Company, and was Deputy United States Trade Representative (1989-1993).

Peter Neumann is Principal Scientist in the Computer Science Laboratory at SRI. He is the Chairman of the ACM Committee on Computers and Public Policy, and a member of the ACM Study Group on crypto policy.

Raymond Ozzie is president of Iris Associates, a wholly-owned subsidiary of the Lotus Development Corporation. Iris Associates is the developer of Lotus Notes.

Kumar Patel is Vice Chancellor for Research at UCLA.

Edward Schmults, retired, was Deputy Attorney General (1981-1984) and a former Senior Vice President for External Relations and General Counsel for the GTE Corporation.

Elliot Stone is Executive Director of the Massachusetts Health Data Consortium which is responsible for the collection and analysis of the state's large health care databases.

Willis Ware, retired, is with RAND Corporation as senior computer scientist emeritus. He chairs the statutory (Computer Security Act) Computer System Security and Privacy Advisory Board.

**Remarks for
Mr. Keith Hall, DASD(I&S)
on the
NRC's Study of National Cryptography Policy
7 October 1994**

NOTE:

Your comments are in *italic*.
NRC Study Team issues are in **block style type**.

● *On behalf of Dr. John Deutch, the Deputy Secretary of Defense, I am pleased to welcome you to Washington, and honored to be here to address the NRC's National Cryptography Policy Study Team.*

● *In its 1991 Publication "Computers at Risk," the National Research Council noted that: "... the Government's efforts [in securing its information infrastructure] have been hamstrung by internecine conflict and underfunding." The NRC continued by stating: "These problems currently appear to be exacerbated, at precisely the time that decisive and concerted action is needed. A coherent strategy must be developed now, given the time, resources, planning, and coordination required to achieve adequate system security and trustworthiness."*

● *For its part the Department is reviewing its ability to provide additional resources designed to secure a significant portion of the Defense Information Infrastructure from attack.*

● *In studying national cryptography policy, you have been charged with developing policy recommendations in arguably the most strategically important, technologically dynamic, difficult and complex subject areas in the Defense arena. In addressing them I suggest to you that the Defense Department is not "... **on the outside looking in**" on your study.*

● *We have a stake in every facet of your study:*

 ~ as customers of cryptography, to include Key Escrow technologies,

~ as being increasingly dependent on the Public Switched Network/National Information Infrastructure,

~ and as the Department assigned the responsibility of securing the nation's and the public's freedoms in a rapidly changing "information based" world.

● The Department's stake is not parochial. It is a matter of concern to the American people, for to the extent that our Defense Information Infrastructure is placed at risk, so too are the lives of the Service men and women who serve on our front lines.

~ Accordingly, DoD is committed to working with you, within the government, and with industry in developing and implementing technologies such as Key Escrow and national cryptography policies that enhance the security of the nation, the freedoms of its citizens, and the competitiveness of its industries.

● In defining the Department's perspective on the study, I thought it would be useful to address briefly some of the key provisions of your task, the first being:

The Impact of current and possible restrictions on and standards for cryptographic technology.

● The Department is not in the business of restricting US industry, its citizens, or its technologies. We do not see the competitiveness of US industry as exclusive from, or opposed to, national security interests. Changes in industrial security, for example, are aimed at promoting the concept that sound security is a joint concern of the department and its industrial infrastructure. We are actively developing revised security arrangements that treat this matter as a Defense/Industry partnership.

● Given the diversity and competency of this study team, there are great expectations regarding your ability to develop recommendations which keep industry competitive, and enable the Department and law enforcement agencies to maintain the nation's security, and the safety and privacy of its citizens in an increasingly invasive information age.

The strength of various cryptographic technologies known today and anticipated for commercial and private purposes, and the strengths and weaknesses of current Key Escrow plans.

● *We believe Clipper with its Key Escrow technology provides the strength necessary to protect American communications now and well into the future. I urge you to examine the Government's position and validate its truth.*

Current and anticipated demand for information systems security based on cryptography.

● *This "demand" needs to be confirmed and clearly documented. I have not seen any specific evidence suggesting the size of the potential market share. Although I am aware that certain industry representatives believe it is large, I would be interested in seeing your results. Anecdotal comments regarding the potential for overseas commerce in cryptography can not be a basis for Administration cryptographic policy decisions that could adversely affect Government's ability to protect individual liberties, ensure public safety, and develop timely intelligence on events transpiring throughout an increasingly unstable world. The bottom line on this issue is: The nation cannot afford to trade critical intelligence capabilities and its security for the possibility of increased commerce.*

Your tasks also ask you to assess:

The impact of foreign restrictions on the market for, importation, and use of our cryptographic technologies, and the adequacy of US cryptographic and cryptographic export policies.

~ *Given the reality of global connectivity, the Department is very interested in your findings on the formation of foreign cryptographic policies and how they impact upon [foreign] national security equities, the desires of the commercial sector and on private citizens. We will also be interested in any differences you may find between stated policy(ies) and on how the policy(ies) is (are) actually implemented.*

~ *Having determined foreign government cryptographic policies and their actual implementation of them, you will be in a good position to*

accomplish your assessment of the adequacy of our own cryptographic policies in meeting the interests of the Government, business and the public.

How technology now and in the future affects policy for balancing US security, law enforcement, privacy, and commercial interests.

● *I do not need to emphasize the technologically driven nature of the issue. However, I must again emphasize that defense of the nation, law enforcement, and the privacy and safety of US citizens are not (as conventional wisdom and even the wording of the study issue strongly suggests) mutually exclusive interests. In fact, the widely reported concerns of Americans over crime and their safety constitute a very close relationship between our citizens, the law enforcement and national security communities. Far from being against measures designed to enhance their security, safety, and privacy, Americans are for them.*

● *Discuss the need for cryptographic technologies and policies that help to secure the National Information Infrastructure in an increasingly interconnected world. The Department and the nation's security, economic health, our standard of living, the safety and freedoms of our people are increasingly dependent on the security of the NII.*

● *Key Escrow does not signal the arrival of "Big Brother." As recent INTERNET break-ins illustrate, "big brothers," not identifiable or subject to US laws, are currently active and are "into" your lives. Unless checked by security technologies such as CLIPPER and its Key Escrow, these "big brothers" could soon seriously affect the nation's security, your safety, businesses, privacy, and bank accounts.*

● *Because of this, throughout your study efforts take a close look at information as a commodity. Information and data (as used in control systems from building air conditioners, to the air traffic control system, to the national power grid) and its integrity, availability, and accuracy is the key to this nation's way of life -- In short, it is America's lifeblood.*

● *I ask you to consider:*

~ The increasing technological pace of information and digital control systems development. Information and data technologies are rapidly becoming ubiquitous.

~ The domination of information workers over those in the manufacturing sector.

~ Mobile/cellular communications and electronic leashes (pagers)

~ All held together by an increasingly vulnerable/high-value/high payoff target -- the nation's public switched network.

● Information, and the systems in which it is processed, has had profound effects on warfighting. The very essence of war and national security is being transformed as I speak.

~ **National Strength:** Has transformed from Industrial/Economic Supremacy to Information Supremacy

~ **Threats to the nation:** Have transformed from Superpowers and Regional powers to Supranational and non-government organizations.

~ **Weaponry:** Has transformed from bombs and bullets to bits and bytes/zeros and ones.

~ **Attack planning and execution:** Has transitioned from months, weeks, and hours to hours, minutes, and seconds.

~ **Command and Control:** Has transformed from organic military and driven by military requirements, to Industrial based/COTS and driven by the marketplace.

~ **Enemy Objectives:** Have transformed from Damage to C2 systems and forward deployed US Forces to Damage, corruption, and destruction of the domestic infrastructure.

~ **Attacks:** Have transitioned from wartime to continuous.

~ *Attackers: Have transitioned from well defined/known adversaries to anyone -- any group -- any nation.*

● *Keep in mind the international nature of Information Warfare (INFOWAR) activities. The ability to wage devastating Information Warfare attacks against a nation like ours -- increasingly dependent on its information systems and supporting public infrastructure -- does not require superpower status. Bear in mind:*

~ *The ability to wage INFOWAR to deny, deceive and/or exploit information and the systems in which they reside, is not restricted to economic superpowers. Through global communications people, interest groups, and nations without great resources can currently safely play very destructive and theoretically decisive roles.*

~ *NSA estimates 95% of all illegal entries into DoD information systems are undetected.*

~ *The need for the United States to maintain Information Warfare and Information System Security superiority.*

● *As a concession to my sense of symmetry, since I began this talk with a quote from the NRC, I feel obligated to close with one from the Joint Security Commission. The quote frames the challenges and responsibilities you shoulder in developing recommendations to guide the development of national cryptography policy, and clearly states the stakes for the nation in the information age.*

~ *"This technology [information warfare] is capable of deciding the outcomes of geopolitical crises without the firing of a single weapon. Our security policies and processes must protect our ability to conduct such infowars while denying the enemy that same advantage."*

● *Again, on behalf of Secretary Deutch, it has been my pleasure to be here -- In the time I have remaining, I would be happy to entertain your questions regarding the Department's perspective on your study.*



ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

November 8, 1994

COMMAND, CONTROL,
COMMUNICATIONS
AND
INTELLIGENCE

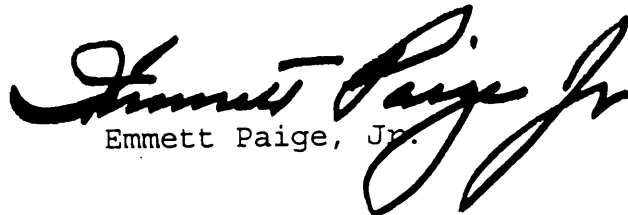
Honorable Dennis DeConcini
Chairman, Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Section 267 of the National Defense Authorization Act for Fiscal Year 1994 directed a 30 month Comprehensive Independent Study of National Cryptography Policy be conducted by the National Research Council (NRC). Accordingly, the NRC's study team held their first meeting on October 7, 1994.

The Department is fully supporting the NRC's efforts. We expect the NRC to complete the study and submit its public report and the classified annex to it not later than May 31, 1997. The Defense Secretary's report to the Committee will follow within 120 days.

Sincerely,


Emmett Paige, Jr.

CC:
Honorable John Warner
Ranking Minority Member



ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

November 8, 1994

COMMAND, CONTROL,
COMMUNICATIONS
AND
INTELLIGENCE

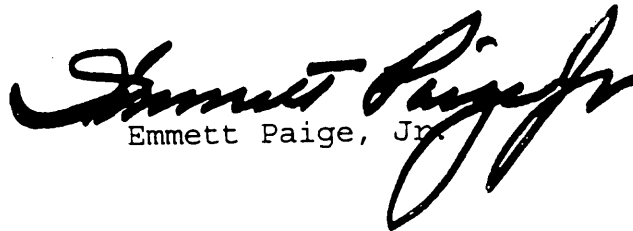
Honorable Joseph Biden Jr.
Chairman, Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Section 267 of the National Defense Authorization Act for Fiscal Year 1994 directed a 30 month Comprehensive Independent Study of National Cryptography Policy be conducted by the National Research Council (NRC). Accordingly, the NRC's study team held their first meeting on October 7, 1994.

The Department is fully supporting the NRC's efforts. We expect the NRC to complete the study and submit its public report and the classified annex to it not later than May 31, 1997. The Defense Secretary's report to the Committee will follow within 120 days.

Sincerely,


Emmett Paige, Jr.

CC:
Honorable Orrin Hatch
Ranking Minority Member



ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

November 8, 1994

COMMAND, CONTROL,
COMMUNICATIONS
AND
INTELLIGENCE

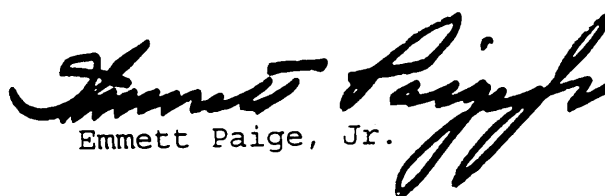
Honorable Sam Nunn
Chairman, Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Section 267 of the National Defense Authorization Act for Fiscal Year 1994 directed a 30 month Comprehensive Independent Study of National Cryptography Policy be conducted by the National Research Council (NRC). Accordingly, the NRC's study team held their first meeting on October 7, 1994.

The Department is fully supporting the NRC's efforts. We expect the NRC to complete the study and submit its public report and the classified annex to it not later than May 31, 1997. The Defense Secretary's report to the Committee will follow within 120 days.

Sincerely,

A handwritten signature in black ink that reads "Emmett Paige, Jr." in a cursive style.

Emmett Paige, Jr.

CC:

Honorable Strom Thurmond
Ranking Minority Member



ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

November 8, 1994

COMMAND, CONTROL,
COMMUNICATIONS
AND
INTELLIGENCE

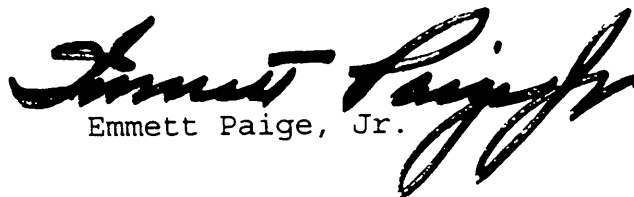
Honorable Jack Brooks
Chairman, Committee on the Judiciary
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Section 267 of the National Defense Authorization Act for Fiscal Year 1994 directed a 30 month Comprehensive Independent Study of National Cryptography Policy be conducted by the National Research Council (NRC). Accordingly, the NRC's study team held their first meeting on October 7, 1994.

The Department is fully supporting the NRC's efforts. We expect the NRC to complete the study and submit its public report and the classified annex to it not later than May 31, 1997. The Defense Secretary's report to the Committee will follow within 120 days.

Sincerely,


Emmett Paige, Jr.

cc:
Honorable Hamilton Fish
Ranking Minority Member



ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

November 8, 1994

COMMAND. CONTROL.
COMMUNICATIONS
AND
INTELLIGENCE

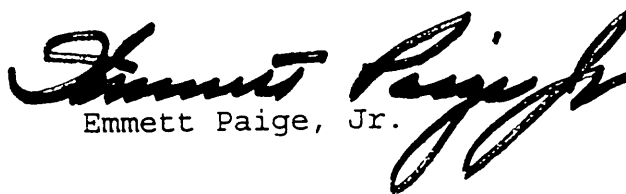
Honorable Dan Glickman
Chairman, Permanent Select
Committee on Intelligence
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Section 267 of the National Defense Authorization Act for Fiscal Year 1994 directed a 30 month Comprehensive Independent Study of National Cryptography Policy be conducted by the National Research Council (NRC). Accordingly, the NRC's study team held their first meeting on October 7, 1994.

The Department is fully supporting the NRC's efforts. We expect the NRC to complete the study and submit its public report and classified annex to it not later than May 31, 1997. The Defense Secretary's report to the Committee will follow within 120 days.

Sincerely,


Emmett Paige, Jr.

cc:
Honorable Larry Combest
Ranking Minority Member



ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

November 8, 1994

COMMAND. CONTROL.
COMMUNICATIONS
AND
INTELLIGENCE

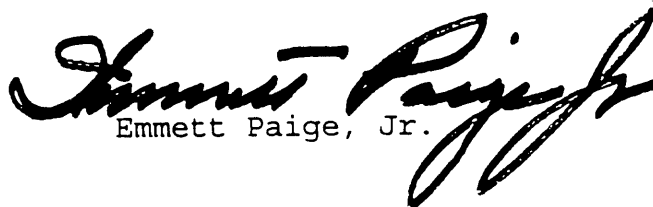
Honorable Ronald V. Dellums
Chairman, Committee on Armed Services
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Section 267 of the National Defense Authorization Act for Fiscal Year 1994 directed a 30 month Comprehensive Independent Study of National Cryptography Policy be conducted by the National Research Council (NRC). Accordingly, the NRC's study team held their first meeting on October 7, 1994.

The Department is fully supporting the NRC's efforts. We expect the NRC to complete the study and submit its public report and the classified annex to it not later than May 31, 1997. The Defense Secretary's report to the Committee will follow within 120 days.

Sincerely,


Emmett Paige, Jr.

CC:

Honorable Floyd D. Spence
Ranking Minority Member



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



22 FEB 1995

MEMORANDUM FOR DIRECTOR, NATIONAL SECURITY AGENCY

SUBJECT: National Research Council Study of National
Cryptography Policy

In the National Defense Authorization Act for Fiscal Year 1994 (Section 267) Congress directed that the National Research Council (NRC) conduct a comprehensive independent study of cryptographic technologies and national cryptography policy.

The NRC is currently under contract to the Department and has initiated their data collection activities. The successful accomplishment of this study effort will require the Department's full cooperation. I am, therefore, requesting that you identify an agency point of contact (POC) to serve as a facilitator for the NRC's efforts. By establishing a direct line of communications between your agency and the NRC, we can assist greatly in the development of an informed and useful report.

Please provide the name, title and telephone number of the POC to both Dr. Herb Lin of the NRC and Mrs. Barbara Valeri, the Department's POC who is the Director for Information Systems Security. Dr. Lin can be reached at 202/334-3191. Mrs. Valeri can be reached at 703/695-8705 and is available to answer any questions you have have on this requirement.

28131



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



22 FEB 1995

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: National Research Council Study of National
Cryptography Policy

In the National Defense Authorization Act for Fiscal Year 1994 (Section 267) Congress directed that the National Research Council (NRC) conduct a comprehensive independent study of cryptographic technologies and national cryptography policy.

The NRC is currently under contract to the Department and has initiated their data collection activities. The successful accomplishment of this study effort will require the Department's full cooperation. I am, therefore, requesting that you identify an agency point of contact (POC) to serve as a facilitator for the NRC's efforts. By establishing a direct line of communications between your agency and the NRC, we can assist greatly in the development of an informed and useful report.

Please provide the name, title and telephone number of the POC to both Dr. Herb Lin of the NRC and Mrs. Barbara Valeri, the Department's POC who is the Director for Information Systems Security. Dr. Lin can be reached at 202/334-3191. Mrs. Valeri can be reached at 703/695-8705 and is available to answer any questions you have on this requirement.

28131



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



22 FEB 1995

MEMORANDUM FOR DIRECTOR, ADVANCED RESEARCH PROJECTS AGENCY

SUBJECT: National Research Council Study of National
Cryptography Policy

In the National Defense Authorization Act for Fiscal Year 1994 (Section 267) Congress directed that the National Research Council (NRC) conduct a comprehensive independent study of cryptographic technologies and national cryptography policy.

The NRC is currently under contract to the Department and has initiated their data collection activities. The successful accomplishment of this study effort will require the Department's full cooperation. I am, therefore, requesting that you identify an agency point of contact (POC) to serve as a facilitator for the NRC's efforts. By establishing a direct line of communications between your agency and the NRC, we can assist greatly in the development of an informed and useful report.

Please provide the name, title and telephone number of the POC to both Dr. Herb Lin of the NRC and Mrs. Barbara Valeri, the Department's POC who is the Director for Information Systems Security. Dr. Lin can be reached at 202/334-3191. Mrs. Valeri can be reached at 703/695-8705 and is available to answer any questions you have have on this requirement.

28131



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



29 FEB 1994

Admiral William O. Studeman, U.S. Navy
Acting Director, Central Intelligence Agency
Washington, DC 20515

Dear Admiral Studeman:

In the National Defense Authorization Act for Fiscal Year 1994 (Section 267), Congress directed the Secretary of Defense to request that the National Research Council (NRC) conduct a comprehensive, independent study of cryptographic technologies and national cryptography policy.

The NRC is currently under contract to the Department of Defense for the performance of this study and has initiated their data collection activities. Because the scope of the NRC study involves a wide range of government and private sector activities and perspectives, its successful accomplishment will depend on the full cooperation of departments and agencies outside of the Department of Defense. Therefore, I solicit the Central Intelligence Agency's cooperation in the study and ask that you identify a point of contact (POC) to serve as a facilitator for the NRC's efforts. By establishing a direct line of communications between the appropriate parties within the NRC and the interested government entities, we can assist greatly in the development of an informed and useful report.

Please provide the name, title and telephone number of your POC to both Dr. Herb Lin of the NRC and Mrs. Barbara Valeri, the Department's POC who is the Director for Information Systems Security. Dr. Lin can be reached at 202/334-3191. Mrs. Valeri can be contacted at 703/695-8705 and is available to answer any questions you may have on this request.

Thank you for your assistance in this matter.

Sincerely,

John M. Deutch



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



22 FEB 1995

Honorable Ronald H. Brown
Secretary of Commerce
Herbert C. Hoover Building
14th Street & Constitution Avenue, N.W.
Washington, DC 20230

Dear Mr. Secretary:

In the National Defense Authorization Act for Fiscal Year 1994 (Section 267), Congress directed the Secretary of Defense to request that the National Research Council (NRC) conduct a comprehensive, independent study of cryptographic technologies and national cryptography policy.

The NRC is currently under contract to the Department of Defense for the performance of this study and has initiated their data collection activities. Because the scope of the NRC study involves a wide range of government and private sector activities and perspectives, its successful accomplishment will depend on the full cooperation of departments and agencies outside of the Department of Defense. Therefore, I solicit the Department of Commerce's cooperation in the study and ask that you identify a point of contact (POC) to serve as a facilitator for the NRC's efforts. By establishing a direct line of communications between the appropriate parties within the NRC and the interested government entities, we can assist greatly in the development of an informed and useful report.

Please provide the name, title and telephone number of your POC to both Dr. Herb Lin of the NRC and Mrs. Barbara Valeri, the Department's POC who is the Director for Information Systems Security. Dr. Lin can be reached at 202/334-3191. Mrs. Valeri can be contacted at 703/695-8705 and is available to answer any questions you may have on this request.

Thank you for your assistance in this matter.

Sincerely,

John M. Deutch

28130



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



22 FEB 1994

Honorable Warren Christopher
Secretary Of State
Main State Department Building
2201 C Street, N.W.
Washington, DC 20520

Dear Mr. Secretary:

In the National Defense Authorization Act for Fiscal Year 1994 (Section 267), Congress directed the Secretary of Defense to request that the National Research Council (NRC) conduct a comprehensive, independent study of cryptographic technologies and national cryptography policy.

The NRC is currently under contract to the Department of Defense for the performance of this study and has initiated their data collection activities. Because the scope of the NRC study involves a wide range of government and private sector activities and perspectives, its successful accomplishment will depend on the full cooperation of departments and agencies outside of the Department of Defense. Therefore, I solicit the Department of State's cooperation in the study and ask that you identify a point of contact (POC) to serve as a facilitator for the NRC's efforts. By establishing a direct line of communications between the appropriate parties within the NRC and the interested government entities, we can assist greatly in the development of an informed and useful report.

Please provide the name, title and telephone number of your POC to both Dr. Herb Lin of the NRC and Mrs. Barbara Valeri, the Department's POC who is the Director for Information Systems Security. Dr. Lin can be reached at 202/334-3191. Mrs. Valeri can be contacted at 703/695-8705 and is available to answer any questions you may have on this request.

Thank you for your assistance in this matter.

Sincerely,

John M. Deutch



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



22 FEB 1995

Honorable Hazel R. O'Leary
Secretary of Energy
Forrestal Building
1000 Independence Avenue, S.W.
Washington, DC 20585

Dear Madame Secretary:

In the National Defense Authorization Act for Fiscal Year 1994 (Section 267), Congress directed the Secretary of Defense to request that the National Research Council (NRC) conduct a comprehensive, independent study of cryptographic technologies and national cryptography policy.

The NRC is currently under contract to the Department of Defense for the performance of this study and has initiated their data collection activities. Because the scope of the NRC study involves a wide range of government and private sector activities and perspectives, its successful accomplishment will depend on the full cooperation of departments and agencies outside of the Department of Defense. Therefore, I solicit the Department of Energy's cooperation in the study and ask that you identify a point of contact (POC) to serve as a facilitator for the NRC's efforts. By establishing a direct line of communications between the appropriate parties within the NRC and the interested government entities, we can assist greatly in the development of an informed and useful report.

Please provide the name, title and telephone number of your POC to both Dr. Herb Lin of the NRC and Mrs. Barbara Valeri, the Department's POC who is the Director for Information Systems Security. Dr. Lin can be reached at 202/334-3191. Mrs. Valeri can be contacted at 703/695-8705 and is available to answer any questions you may have on this request.

Thank you for your assistance in this matter.

Sincerely,


John M. Deutch



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



22 FEB 1995

Honorable Janet Reno
Attorney General of the United States
Main Justice Building
10th Street & Constitution Avenue, N.W.
Washington, DC 20530

Dear Madame Attorney General:

In the National Defense Authorization Act for Fiscal Year 1994 (Section 267), Congress directed the Secretary of Defense to request that the National Research Council (NRC) conduct a comprehensive, independent study of cryptographic technologies and national cryptography policy.

The NRC is currently under contract to the Department of Defense for the performance of this study and has initiated their data collection activities. Because the scope of the NRC study involves a wide range of government and private sector activities and perspectives, its successful accomplishment will depend on the full cooperation of departments and agencies outside of the Department of Defense. Therefore, I solicit the Department of Justice's cooperation in the study and ask that you identify a point of contact (POC) to serve as a facilitator for the NRC's efforts. By establishing a direct line of communications between the appropriate parties within the NRC and the interested government entities, we can assist greatly in the development of an informed and useful report.

Please provide the name, title and telephone number of your POC to both Dr. Herb Lin of the NRC and Mrs. Barbara Valeri, the Department's POC who is the Director for Information Systems Security. Dr. Lin can be reached at 202/334-3191. Mrs. Valeri can be contacted at 703/695-8705 and is available to answer any questions you may have on this request.

Thank you for your assistance in this matter.

Sincerely,

John M. Deutch



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010



22 FEB 1995

Honorable Robert E. Rubin
Secretary of the Treasury
Main Treasury
1500 Pennsylvania Avenue, N.W.
Washington, DC 20220

Dear Mr. Secretary:

In the National Defense Authorization Act for Fiscal Year 1994 (Section 267), Congress directed the Secretary of Defense to request that the National Research Council (NRC) conduct a comprehensive, independent study of cryptographic technologies and national cryptography policy.

The NRC is currently under contract to the Department of Defense for the performance of this study and has initiated their data collection activities. Because the scope of the NRC study involves a wide range of government and private sector activities and perspectives, its successful accomplishment will depend on the full cooperation of departments and agencies outside of the Department of Defense. Therefore, I solicit the Department of Treasury's cooperation in the study and ask that you identify a point of contact (POC) to serve as a facilitator for the NRC's efforts. By establishing a direct line of communications between the appropriate parties within the NRC and the interested government entities, we can assist greatly in the development of an informed and useful report.

Please provide the name, title and telephone number of your POC to both Dr. Herb Lin of the NRC and Mrs. Barbara Valeri, the Department's POC who is the Director for Information Systems Security. Dr. Lin can be reached at 202/334-3191. Mrs. Valeri can be contacted at 703/695-8705 and is available to answer any questions you may have on this request.

Thank you for your assistance in this matter.

Sincerely,

John M. Deutch

NATIONAL ACADEMY OF SCIENCES

2101 Constitution Avenue

Washington, DC 20418

OFFICE OF CONTRACTS AND GRANTS
FAX: (202) 334-2797

OFFICE LOCATION:
Cecil and Ida Green Building
2001 Wisconsin Avenue NW, Room GR406

May 20, 1994

Ms. Barbara L. Valeri
Director of Information Systems Security
Office of the Assistant Secretary of Defense
Washington, DC 20301-3040

RE: Proposal No. 94-154-01; "National Cryptography Policy"

Dear Ms. Valeri:

This letter is in response to the recommended changes and requests for clarification contained in Enclosure 1 of your letter of May 2, 1994. The responses are numbered to coincide with the numbers of the points made in your letter; responses have been prepared by Mr. Herb Lin of the Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications.

- 1 a. The NRC has established through the Chief of the Office of Naval Research a cadre of SCI billets for those committee members and staff necessary to conduct the study. Nominations to receive SCI clearances will be limited to those individuals with a strict "need-to-know". Individuals requiring access to non-SCI classified information have or will be processed for the appropriate level of clearance through the Defense Industrial Security Clearance Office (DISCO).
- 1 b. A package of names for individuals to receive SCI clearances for the study will be forwarded to the Department of Defense as soon as possible. In accordance with Public Law 103-160 (The Defense Authorization Act of FY 1994), it is anticipated that the Department of Defense will expedite to the fullest degree possible the processing of security clearances that are necessary for the National Research Council to conduct the study.
- 1 c. We agree that access to classified data is contingent on the successful completion of required background checks and investigations and the execution of non-disclosure agreements.
- 1 d. The NRC review process entails two separate but related steps to insure the intellectual integrity of NRC reports.
 - + The first step is the review of the draft report by individuals not associated with the study project. These individuals make comments to the NRC that are forwarded to the original study committee. The study committee is required to respond to each and every comment of the reviewers; the result of this response is either an alteration of the manuscript in response to a comment, or a statement that explains why the committee chose not to alter the manuscript.

- + The second step is taken by the NRC's Report Review Committee (RRC). This committee examines the original draft manuscript, all reviewer comments, and the revised manuscript to ensure that the study committee has done an adequate job in responding to reviewer comments. On occasion, the RRC may suggest changes itself. Once the RRC approves a manuscript, it is ready for transmittal to the sponsor.

If the draft report includes classified material, individuals with appropriate security clearances will be selected as reviewers for those sections containing such material.

- 1 e. Not included in your request.
- 1 f. The report will be submitted to the Department of Defense prior to publication in final form for security review to ensure that classified material is not inadvertently disclosed.

2 a through 2 d.

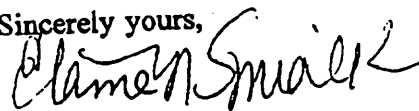
In addition to the items listed on pages 2 and 3 of our proposal under Project Content, the study will also address:

- + current and anticipated demand for information systems security based on cryptography.
- + the impact of foreign restrictions on the use of, importation of, and the market for cryptographic technology.
- + the extent to which current cryptography policy is adequate for protecting U.S. interests in privacy, public safety, national security, and economic competitiveness.
- + technical strengths and weaknesses of current key escrow implementation schemes.

3. While there are currently no restrictions on the American use of encryption, the impact of possible restrictions on such use on the competitiveness and performance of commercial U.S. users is a matter of some concern within the community. It is thus an appropriate point for the project to consider.

If you have questions regarding the foregoing, or require further clarification, please contact me at (202) 334-3178. We look forward to working with you on this worthwhile project.

Sincerely yours,



Elaine M. Smialek
Contract Manager

cc: H. Lin
M. Blumenthal



COMMAND CONTROL
COMMUNICATIONS
AND INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-3040

2 MAY 1994

Ms. Elaine M. Smilek
Contract Manager, Office of
Contracts and Grants
National Academy of Sciences
2101 Constitution Avenue
Washington, D.C. 20301-6000

Dear Ms. Smilek,

The Department of Defense has completed its review of your Statement of Work (SOW), Proposal No. 94-CPSMA-154, for a 32 Month study entitled "*National Cryptography Policy*." Recommended changes to the SOW and requests for clarification are provided in Enclosure 1. I believe the changes offered will satisfactorily address the security concerns of the Department and help promote the development of a highly useful product. The Department is prepared to proceed with the study upon agreement on the SOW provisions. I would be happy to meet with you and other staff members to facilitate this process.

My action officers for the study are Messrs. William Freestone and Jeff Gaynor. They can be contacted at: (703) 602-5878 and 602-5876 respectively.

Sincerely,

A handwritten signature in black ink, appearing to read "Barbara L. Valeri", with a horizontal line underneath.

Barbara L. Valeri
Director of Information Systems Security

Enclosure

Review of the National Research Council Statement of Work
Study Proposal Number 94-CPSMA-154
"National Cryptography Policy"

1. The proposed study will require access to extremely sensitive information, the divulgence of which could cause grave damage to the nation's security. Accordingly, the following security specifications should be added to the Statement of Work (SOW) to bring the study into compliance with national regulations for the handling of Special Intelligence and cryptographic information.

a. The SOW contemplates the clearing of up to 5 panel members for access to Sensitive Compartmented Information (SCI). Inasmuch as the panel will require administrative support, the number of panel members cleared to SCI should be limited to three with a similar number of administrative/clerical personnel being cleared to the same level.

b. The SOW should specify when security clearance applications will be submitted.

c. The SOW should include a provision that access to classified data is contingent on the successful completion of required background checks and investigations, and the execution of non-disclosure agreements.

d. The SOW makes reference to NRC "review procedures." Materials describing the procedures should be forwarded to this office for review in order for the Department to determine if they are appropriate in the context of the proposed study. Once approved, include the review procedures in the SOW.

f. Include in the SOW a provision which requires submission of the report to DoD for security review (to prevent inadvertent disclosures of classified information), before the study is published in final form.

2. The Project Content portion of the SOW should include the NRC's study of:

a. Current and anticipated demand for information systems security.

b. The impact of foreign restrictions on the use of, and market for, cryptographic technology.

● NOTE: Many countries impose restrictions on the cryptography that may be imported into their countries or connected to their public switched networks. This suggests that a "free market" for encryption may never exist. This could be a significant factor in projecting future markets.

Enclosure 1

c. The extent to which current cryptographic policy satisfies the interests of privacy, public safety, national security, and competitiveness. In doing so, reviewers will be able to compare what the policy is doing well and what it is not.

d. Alternatives to current key escrow implementation. The study should specifically address whether key escrow encryption can be implemented in software with assurance that communications will be secured, and that the key escrow mechanism can not be bypassed.

3. The Project Content section of the SOW includes a provision that appears to reflect a misunderstanding of current regulations. Since there are no U.S. imposed restrictions on U.S. user use of encryption, here or abroad, query the rationale for studying the impact of restrictions on *"the competitiveness and performance of commercial US users of such technology."*

Comparison of the National Research Council Response
to DoD ISS Letter of 2 May 1994
Study Proposal Number 94-CPSMA-154
"National Cryptography Policy"

The NRC has responded to our 2 May 1994 letter. Below is an analysis of their response to the issues raised in our letter and a copy of their response.

ISS Letter - Paragraph 1a: The SOW contemplates the clearing of up to 5 panel members for access to Sensitive Compartmented Information (SCI). Inasmuch as the panel will require administrative support, the number of panel members cleared to SCI should be limited to three with a similar number of administrative/clerical personnel being cleared to the same level.

NRC Response Analysis: NRC notes SCI billets for the NRC are maintained by the Office of Naval Research. The NRC will decide how many and of what variety (panel members or administrative) of people are cleared for access to SCI on a strict "need-to-know" basis. Individuals requiring non-SCI access will be processed through DISCO.

ISS Letter - Paragraph 1b: The SOW should specify when security clearance applications will be submitted.

NRC Response Analysis: Clearance packages will be forwarded to DoD ASAP. NRC notes "... in accordance with Public Law 103-160 (Defense Authorization Act of FY 1994) it is anticipated we will to the fullest degree possible expedite the processing of security clearances for the study.

ISS Letter - Paragraph 1c: The SOW should include a provision that access to classified data is contingent on the successful completion of required background checks and investigations, and the execution of non-disclosure agreements.

NRC Response Analysis: Concur.

ISS Letter - Paragraph 1d: The SOW makes reference to NRC "review procedures." Materials describing the procedures should be forwarded to this office for review in order for the Department to determine if they are appropriate in the context of the proposed study. Once approved, include the review procedures in the SOW.

NRC Response Analysis: NRC provided the "two separate steps" of their "Review Procedures." They are designed to "...ensure the intellectual integrity of NRC reports." As such, the steps have nothing to do with the security concerns or damage to national security raised by us in item 1d.

The NRC does note that individuals with security clearances will review (ostensibly for "intellectual integrity") any classified portions of the study. Regardless, the question of NRC security review procedures remains unanswered.

ISS Letter - Paragraph 1f: Include in the SOW a provision which requires submission of the report to DoD for security review (to prevent inadvertent disclosures of classified information), before the study is published in final form.

NRC Response Analysis: Concur.

ISS Letter - Paragraphs 2a through 2d: The Project Content portion of the SOW should include the NRC's study of:

a. Current and anticipated demand for information systems security. •

b. The impact of foreign restrictions on the use of, and market for, cryptographic technology.

• NOTE: Many countries impose restrictions on the cryptography that may be imported into their countries or connected to their public switched networks. This suggests that a "free market" for encryption may never exist. This could be a significant factor in projecting future markets.

c. The extent to which current cryptographic policy satisfies the interests of privacy, public safety, national security, and competitiveness. In doing so, reviewers will be able to compare what the policy is doing well and what it is not.

d. Alternatives to current key escrow implementation. Specifically address, the question: If the encryption algorithm resides in software, can key escrow be implemented with assurance that communications will be secured, and that the key escrow mechanism can not be bypassed?

NRC Response Analysis: Concur. The above items will be included in the study.

ISS Letter - Paragraph 3: The Project Content section of the SOW includes a provision that appears to reflect a misunderstanding of current regulations. Since there are no U.S. imposed restrictions on U.S. user use of encryption, here or abroad, query the rationale for studying the impact of restrictions on "the competitiveness and performance of commercial US users of such technology."

NRC Response Analysis: While there are currently no restrictions on the American use of encryption, the impact of possible restrictions "... is a matter of some concern within the community." Thus the topic will be covered in the study.

ISS Bottom Line: The NRC has attempted to meet most of our study requirements. However, from its response to our paragraph 1d, it appears the NRC lacks formal in-house security "*review procedures.*" Recommend this issue be raised with the NRC in subsequent correspondence and that the study not be allowed to proceed until NRC security procedures for this study are approved by DoD and included in the SOW.

AWARD / CONTRACT

THIS CONTRACT IS A RATED ORDER
UNDER DPAS (15CFR 350)

RAT

PAGE OF P.

2. CONTRACT (Proc. Inst. Ident.) NO. DASW01-94-C-0178		3. EFFECTIVE DATE 09/30/94		4. REQUISITION/PURCHASE REQUEST/PROJECT NO. H91268-4201-0020	
5. ISSUED BY DEFENSE SUPPLY SERVICE - WASHINGTON 5200 ARMY PENTAGON WASHINGTON, DC 20310-5200 ROBERT J. LAVELLE RJL (703) 614-4578		CODE I A74V8H		5. ADMINISTERED BY (if other than item 5) DNRRR 101 MARIETTA TOWER SUITE 2805 ATLANTA, GA 30303	

7. NAME AND ADDRESS OF CONTRACTOR (No. street, city, county, State and ZIP Code) NATIONAL ACADEMY OF SCIENCES 2101 CONSTITUTION AVENUE WASHINGTON DC 20418		Vendor ID: 00003762		8. DELIVERY <input type="checkbox"/> FOB ORIGIN <input checked="" type="checkbox"/> OTHER (See below)	
				9. DISCOUNT FOR PROMPT PAYMENT 00.000% 00 Net 030	
				10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN: ITEM ARTICLE G-2	

CODE 10969		FACILITY CODE		11. SHIP TO/MARK FOR IN ACCORDANCE WITH ARTICLE F-3	
11. SHIP TO/MARK FOR IN ACCORDANCE WITH ARTICLE F-3		CODE SEESCHED		12. PAYMENT WILL BE MADE BY DFAS CODE 40, ROOM 406, CRYSTAL MALL #3 WASHINGTON, DC 20371	

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION <input checked="" type="checkbox"/> 10 U.S.C. 2304(e)(1) (5) <input type="checkbox"/> 41 U.S.C. 253(c)		14. ACCOUNTING AND APPROPRIATION DATA ACRN AA: 9740400.4500 544E51 999-2500 S18119 02380000 IX 0000 X6101A Award Oblig Amt US\$ 400,000.00			
--	--	---	--	--	--

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	COST REIMBURSEMENT (NO FEE) CONTRACT See attached Schedule(s)				

15G. TOTAL AMOUNT OF CONTRACT **B** 798,735.00

(X) SEC.	DESCRIPTION	PAGE (S)	(X) SEC.	DESCRIPTION	PAGE (S)
PART I - THE SCHEDULE			PART II - CONTRACT CLAUSES		
X	A	SOLICITATION/CONTRACT FORM	X	I	CONTRACT CLAUSES
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS			9
PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.					
X	C	DESCRIPTION/SPECS./WORK STATEMENT	X	J	LIST OF ATTACHMENTS
X	D	PACKAGING AND MARKING			1
PART IV - REPRESENTATIONS AND INSTRUCTIONS					
X	E	INSPECTION AND ACCEPTANCE		K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS
X	F	DELIVERIES OR PERFORMANCE		L	INSTRS., CONDS., AND NOTICES TO OFFERORS
X	G	CONTRACT ADMINISTRATION DATA		M	EVALUATION FACTORS FOR AWARD
X	H	SPECIAL CONTRACT REQUIREMENTS			

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. <input checked="" type="checkbox"/> CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return ORIGINAL copies to issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award / contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)		18. <input type="checkbox"/> AWARD (Contractor is not required to sign this document.) Your offer on Solicitation Number _____ including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your offer, and (b) this award / contract. No further contractual document is necessary.	
--	--	---	--

19A. NAME AND TITLE OF SIGNER (Type or print) MARY PAT RUKAWA, Director Office of Contracts and Grants		20A. NAME OF CONTRACTING OFFICER HARRY W. SHATTO, JR. HWS (703) 614-4579	
19B. NAME OF CONTRACTOR (Signature of person authorized to sign)		20B. UNITED STATES OF AMERICA BY <i>Harry W. Shatto, Jr.</i> (Signature of Contracting Officer)	
19C. DATE SIGNED SEP 30 1994		20C. DATE SIGNED SEP 30	

SECTION 8
SUPPLIES OR SERVICES AND PRICES/COSTS

Pursuant to Section 267 of the National Defense Authorization Act for Fiscal Year 1994, a study shall be conducted by the National Research Council of the National Academy of Sciences (Contractor).

The study entitled: "Comprehensive Independent Study of National Cryptographic shall assess:

(1) The effect of cryptographic technologies on: National security interests of the United States Government, Law enforcement interests of the United States Government, Commercial interests of United States industry, Privacy interests of United States citizens; and

(2) The effect on commercial interests of United States industry of export controls on cryptographic technologies.

ITEM	DESCRIPTION	QUANTITY	U/I	UNIT PRICE	AMOUNT
0001	"Comprehensive Independent Study of National Cryptographic Policy"	1.00	LT	798735.000000	798,735.00
0002	Reports and Other Deliverables	1.00	LT	NSP	
0002AA	MEETINGS (Committee, Dissemination, and Staff)	As Required		NSP	
0002AB	FINAL REPORT (In accordance with the PRODUCT AND DISSEMINATION PLAN, as set forth in the Contractor's proposal).	1.00	LT	NSP	

TOTAL ESTIMATED COST: \$ 798,735.00
END OF SECTION 8

SECTION C
DESCRIPTION/SPECS./WORK STATEMENT

C-1. INCORPORATION OF TECHNICAL PROPOSAL

Contractor shall furnish the necessary personnel, materials, facilities, and other supplies/services as specified in its technical proposal entitled: "National Cryptography Policy" (Original - dated March 1994; Revised - dated June 1994). The technical proposal, as revised, is hereby incorporated at SECTION J, Attachment #1.

C-2. ENGLISH LANGUAGE DOCUMENTATION

All Contractor-prepared material to be furnished under this contract shall be written in the English language, and all measurements shall be in the English Linear measure and avoirdupois weight systems.

END OF SECTION C

SECTION D
PACKAGING AND MARKING

D.1 METHOD OF TRANSMISSION (TOP SECRET)

Top secret material may be transmitted by (i) a specifically designated escort or courier cleared for access to TOP SECRET information (military, US civilian employee, or a responsible employee designated by the contractor, except the contractor's employee shall not carry classified material across international boundaries) or, (ii) Armed Forces Courier services using a contractor assigned ARFCOS account number. Under no circumstances shall TOP SECRET material be transmitted through the US or company mail channels.

D.2 PACKAGING AND MARKING OF CLASSIFIED ITEMS

(a) CONFIDENTIAL or SECRET material will be packed to conceal it properly and to avoid suspicion as to contents, and to reach destination in satisfactory condition. Internal markings or internal packaging will clearly indicate the classification. NO NOTATION TO INDICATE CLASSIFICATION WILL APPEAR IN EXTERNAL MARKINGS. (See paragraph 17 of the Industrial Security Manual for Safeguarding Classified Information, DoD 5220.22-M.)

(b) CONFIDENTIAL or SECRET documents will be enclosed in two (2) opaque envelopes or covers. The inner envelope or cover containing the documents being transmitted will be addressed, return addressed and sealed. The classification of the documents being transmitted will be clearly marked on the front and back of the inner container. The classified documents will be protected from direct contact with the inner cover by a cover sheet or by folding inward. For SECRET documents, a receipt form identifying the addresser, addressee and documents will be enclosed in the inner envelope. CONFIDENTIAL documents will be covered by a receipt only when the sender deems it necessary. The inner envelope or cover will be enclosed in an opaque outer envelope or cover. The classification markings of the inner envelope should not be detectable. The outer envelope will be addressed, return addressed and sealed. NO CLASSIFICATION MARKINGS WILL APPEAR ON THE OUTER ENVELOPE OR COVER.

END OF SECTION D

SECTION E
INSPECTION AND ACCEPTANCE

- E.1 52.246-9 INSPECTION OF RESEARCH AND DEVELOPMENT (SHORT FORM) (APR 1984)
(Reference 46.309)
- E.2 252.246-7000 MATERIAL INSPECTION AND RECEIVING REPORT (DEC 1991)
(Reference 46.370)

END OF SECTION E

SECTION F
DELIVERIES OR PERFORMANCE

F.1 52.247-34 F.O.B. DESTINATION (NOV 1991)
(Reference 47.303-6(c))

F.2 TERM OF CONTRACT

The term of this contract is from 30 September 1994 through 31 May 1997.

F.3 PLACE OF DELIVERY (COR)

All items to be delivered under this contract shall be delivered to the Contracting Officer's Representative (COR) at the location(s) specified below:

Mr. Jeffrey R. Gaynor (OSD, Director of Information Systems Security) Room 3C-341, The Pentagon Washington, DC 20301-3040.

F.4 REPORTS AND OTHER DELIVERABLES

Delivery of all reports and other deliverables shall be made to the address specified in Section F in accordance with the following:

ITEM NO	DESCRIPTION	DATE (on or Before)
0002AA	Meetings	As required
0002AB	Final Report	In accordance with Contractor Technical Proposal: Product and Dissemination Plan (p/4)

END OF SECTION F

SECTION G
CONTRACT ADMINISTRATION DATA

G.1 252.201-7000 CONTRACTING OFFICER'S REPRESENTATIVE (DEC 1991)

(a) Definition. "Contracting officer's representative" means an individual designated in accordance with subsection 201.602-2 of the Defense Federal Acquisition Regulation Supplement and authorized in writing by the Contracting Officer to perform specific technical or administrative functions.

(b) If the Contracting Officer designates a contracting officer's representative (COR), the Contractor will receive a copy of the written designation. It will specify the extent of the COR's authority to act on behalf of the Contracting Officer. The COR is not authorized to make any commitments or changes that will affect price, quality, quantity, delivery, or any other term or condition of the contract.

(End of clause)

G.2 VOUCHERS

(a) Vouchers, identified by contract number, including delivery order number, if applicable, with supporting statements, shall be submitted for review and provisional approval to the cognizant audit agency listed below:

DCAA - District Branch Office, 8181 Professional Place, Suite 101 Landover, MD 20785-2218

(b) One (1) copy of each voucher shall be mailed to the Contracting Officer's Representative at the address listed below:

Mr. Jeffrey R. Gaynor, (OSD Director of Information Systems Security) Room 3C-841, The Pentagon Washington, DC 20301-3040

G.3 DELEGATION OF AUTHORITY FOR CONTRACT ADMINISTRATION

The following contracting administration office is hereby designated as the authorized representative of the Contracting Officer for the purpose of administering this contract in accordance with current directives:

Office of Naval Resident Research Representative (ONRRR) 101 Marietta
Tower, Suite 2805 Atlanta, GA 30323-0008

G.4

CONTRACTING OFFICER'S REPRESENTATIVE

(a) The Contracting Officer's Representative (COR) under this contract is Mr. Jeffrey R. Gaynor (OSD, Director of Information Systems Security) TELEPHONE: (703) 693-6686 Room 3C-841, The Pentagon Washington, DC 20301-3040.

(b) The Contractor is advised that only the Contracting Officer can change or modify the contract terms or take any other action which obligates the Government. Then, such action must be set forth in a formal modification to the contract. The authority of the COR is strictly limited to the specific duties set forth in his/her letter of appointment, a copy of which is furnished to the Contractor. Contractors who rely on direction from other than the Contracting Officer or a COR acting within the strict limits of his responsibilities as set forth in his/her letter of appointment do so at their own risk and expense. Such actions do not bind the Government contractually. Any contractual questions shall be directed to the Contracting Officer.

END OF SECTION G

SECTION H
SPECIAL CONTRACT REQUIREMENTS

H.1 PAPERWORK REDUCTION ACT

In the event that it becomes necessary to collect information upon identical forms from ten or more persons other than federal employees, the Paperwork Reduction Act shall apply to this contract, and the contractor shall obtain through the COR the required DOD clearance. No funds will be expended or any contracts made for the collection of data from public respondents until the contractor is given written notice by the contracting officer.

H.2 MILITARY SECURITY CLASSIFICATION

Military security requirements in the performance of this contract shall be maintained in accordance with FAR 52.204-2. Security Requirements and the DD Form 254 contained in Section J. The highest classification involved in the performance of this contract is TOP SECRET. This contract document is UNCLASSIFIED. All individuals requiring access to collateral information in connection with this contract will be processed for the appropriate level of clearance through the Defense Industrial Clearance Office (DISCO). Cleared individuals will also be required to comply with all security practices, procedures, and regulations to prevent loss or compromise of classified national security information.

H.3 INCORPORATION OF CERTIFICATIONS

Section K, "Representations, Certifications and Other Statements of Offerors", Section L, "Instructions, Conditions, and Notices to Offerors or Bidders", and Section M, "Evaluation Factors for Award", although withdrawn at time of award, are hereby incorporated by reference with the same force and effect as if stated in full text.

H.4 SPECIAL ACCESS AND COMPETITIVE PROCUREMENT

(a) Proprietary Data of Third Parties. In the event the Contractor

requests access to proprietary data of other companies, in order to conduct studies and research under the contract, it will enter into agreements with the supplying companies to protect such data from unauthorized use or disclosure so long as such data remains proprietary.

(b) Proprietary Data Furnished by the Government. In the event the Contractor is given access by the Government to proprietary data of the Government or proprietary data of third parties possessed by the Government, the Contractor hereby agrees to protect such data from unauthorized use or disclosure as long as such data remains proprietary.

H.5

PRE-CONTRACT COSTS

All costs incurred on or after 21 JULY, 1994 by the contractor in anticipation of this contract, which if incurred after the effective date of this contract would have been considered allowable costs hereunder, shall be allowable costs hereunder; provided, however, such costs shall not exceed \$50,000.00.

H.6

INCREMENTAL FUNDING

This contract shall be subject to incremental funding, with \$ 400,000.00 presently available for performance. It is estimated that the funds presently available are sufficient to permit the contractor's performance through 30 September, 1995. In accordance with the Section 10 clauses "Termination" and "Limitation of Funds," no legal liability on the part of the Government for payment of money in excess of \$ 400,000.00 shall arise unless and until additional funds are made available by the Contracting Officer through a modification of this contract.

H.7

ALLOWABLE COSTS

For the term of this contract, the Contractor will be reimbursed for allowable costs in accordance with FAR Subpart 31.2.

H.8

CONTRACTOR VISITS

At the request of the Contractor, the Contracting Officer's Representative (COR) will coordinate Contractor visits to a sponsor's agency and other DoD agencies necessary for performance under this contract.

SECTION I
CONTRACT CLAUSES

I.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (JUN 1988)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

(End of clause)

- I.2 52.202-1 DEFINITIONS (SEPT 1991)
(Reference 2.201)
- I.3 52.203-1 OFFICIALS NOT TO BENEFIT (APR 1984)
(Reference 3.102-2)
- I.4 52.203-3 GRATUITIES (APR 1984)
(Reference 3.202)
- I.5 52.203-5 COVENANT AGAINST CONTINGENT FEES (APR 1984)
(Reference 3.404(c))
- I.6 52.203-7 ANTI-KICKBACK PROCEDURES (OCT 1988)
(Reference 3.502-3)
- I.7 52.203-10 PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY (SEP 1990)
(Reference 3.104-10(c))
- I.8 52.203-12 LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (JAN 1990)
(Reference 3.808(b))
- I.9 52.204-2 SECURITY REQUIREMENTS (APR 1984)
(Reference 4.404(a))
- I.10 52.209-6 PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT (NOV 1992)
(Reference 9.409(b))
- I.11 52.215-1 EXAMINATION OF RECORDS BY COMPTROLLER GENERAL (FEB 1993)
(Reference 15.106-1(b))
- I.12 52.215-22 PRICE REDUCTION FOR DEFECTIVE COST OR PRICING DATA (JAN 1991)
(Reference 15.804-8(a))

- I.13 52.215-23 PRICE REDUCTION FOR DEFECTIVE COST OR PRICING DATA--MODIFICATIONS
(DEC 1991)
(Reference 15.804-8(b))
- I.14 52.215-27 TERMINATION OF DEFINED BENEFIT PENSION PLANS (SEP 1989)
(Reference 15.804-8(e))
- I.15 52.215-30 FACILITIES CAPITAL COST OF MONEY (SEP 1987)
(Reference 15.904(a))
- I.16 52.215-33 ORDER OF PRECEDENCE (JAN 1986)
(Reference 15.406-3(b))
- I.17 52.215-39 REVERSION OR ADJUSTMENT OF PLANS FOR POSTRETIREMENT BENEFITS OTHER THAN
PENSIONS (PRB) (JUL 1991)
(Reference 15.804-8(f))
- I.18 52.216-7 ALLOWABLE COST AND PAYMENT (JUL 1991)
(Reference 16.307(a))
- I.19 52.216-11 I COST CONTRACT--NO FEE (APR 1984)--ALTERNATE I (APR 1984)
(Reference 16.307(e)(2))
- I.20 52.216-15 PREDETERMINED INDIRECT COST RATES (APR 1984)
(Reference 16.307(1))
- I.21 52.222-26 EQUAL OPPORTUNITY (APR 1984)
(Reference 22.810(e))
- I.22 52.222-35 AFFIRMATIVE ACTION FOR SPECIAL DISABLED AND VIETNAM ERA VETERANS
(APR 1984)
(Reference 22.1305(a)(1))
- I.23 52.222-36 AFFIRMATIVE ACTION FOR HANDICAPPED WORKERS (APR 1984)
(Reference 22.1408(a))
- I.24 52.222-37 EMPLOYMENT REPORTS ON SPECIAL DISABLED VETERANS AND VETERANS OF THE
VIETNAM ERA (JAN 1988)
(Reference 22.1308(b))

I.25 52.223-2 CLEAN AIR AND WATER (APR 1984)
(Reference 23.105(b))

I.26 52.223-6 DRUG-FREE WORKPLACE (JUL 1990)
(Reference 23.505(b))

I.27 52.227-14 RIGHTS IN DATA--GENERAL (JUN 1987)
(Reference 27.409(a)(1))

I.28 52.227-21 TECHNICAL DATA CERTIFICATION, REVISION, AND WITHHOLDING OF PAYMENT--
MAJOR SYSTEMS (JUN 1987)
(Reference 27.409(a))

I.29 52.230-3 DISCLOSURE AND CONSISTENCY OF COST ACCOUNTING PRACTICES (AUG 1992)
(Reference 30.201-4(b))

I.30 52.230-4 CONSISTENCY IN COST ACCOUNTING PRACTICES (AUG 1992)
(Reference 30.201-4(c))

I.31 52.230-5 ADMINISTRATION OF COST ACCOUNTING STANDARDS (AUG 1992)
(Reference 30.201-4(d))

I.32 52.232-9 LIMITATION ON WITHHOLDING OF PAYMENTS (APR 1984)
(Reference 32.111(c)(2))

I.33 52.232-22 LIMITATION OF FUNDS (APR 1984)
(Reference 32.705-2(c))

I.34 52.232-23 ASSIGNMENT OF CLAIMS (JAN 1986)
(Reference 32.906(a)(1))

I.35 52.232-25 PROMPT PAYMENT (MAR 1994)
(Reference 32.908(c))

I.36 52.232-28 ELECTRONIC FUNDS TRANSFER PAYMENT METHODS (APR 1989)
(Reference 32.908(d))

I.37 52.233-1 I DISPUTES (MAR 1994)--ALTERNATE I (DEC 1991)
(Reference 33.215)

I.38 52.233-3 I PROTEST AFTER AWARD (JUN 1985)--ALTERNATE I (JUN 1985)
(Reference 33.106(b))

- I.39 52.242-1 NOTICE OF INTENT TO DISALLOW COSTS (APR 1984)
(Reference 42.802)
- I.40 52.243-2 V CHANGES--COST-REIMBURSEMENT (AUG 1987)--ALTERNATE V (APR 1984)
(Reference 43.205(b)(6))
- I.41 52.246-25 LIMITATION OF LIABILITY--SERVICES (APR 1984)
(Reference 46.805(a)(4))
- I.42 52.249-5 TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (EDUCATIONAL AND OTHER
NONPROFIT INSTITUTIONS) (APR 1984)
(Reference 49.502(d))
- I.43 252.203-7000 STATUTORY PROHIBITION ON COMPENSATION TO FORMER DEPARTMENT OF DEFENSE
EMPLOYEES (DEC 1991)
(Reference 03.170-4)
- I.44 252.203-7001 SPECIAL PROHIBITION ON EMPLOYMENT (APR 1993)
(Reference)
- I.45 252.203-7003 PROHIBITION AGAINST RETALIATORY PERSONNEL ACTIONS (APR 1992)
(Reference 03.7108)
- I.46 252.215-7000 PRICING ADJUSTMENTS (DEC 1991)
(Reference 15.804-8(1))
- I.47 252.223-7004 DRUG-FREE WORK FORCE (SEP 1988)
(Reference 23.570-4)
- I.48 252.227-7018 RESTRICTIVE MARKINGS ON TECHNICAL DATA (OCT 1988)
(Reference 27.403-72(a))
- I.49 252.227-7029 IDENTIFICATION OF TECHNICAL DATA (APR 1988)
(Reference 27.403-72(a))
- I.50 252.227-7030 TECHNICAL DATA--WITHHOLDING OF PAYMENT (OCT 1988)
(Reference 27.403-74(b))
- I.51 252.227-7037 VALIDATION OF RESTRICTIVE MARKINGS ON TECHNICAL DATA (APR 1988)
(Reference 27.403-73(a))

- I. 52 252.231-7000 SUPPLEMENTAL COST PRINCIPLES (DEC 1991)
(Reference 31.100-70) .
- I. 53 252.231-7001 PENALTIES FOR UNALLOWABLE COSTS (MAY 1994)
(Reference)
- I. 54 252.232-7005 REIMBURSEMENT OF SUBCONTRACTOR ADVANCE PAYMENTS--DOD PILOT MENTOR-PROTEGE
PROGRAM (DEC 1991)
(Reference 32.412-70(c)
- I. 55 252.233-7000 CERTIFICATION OF CLAIMS AND REQUESTS FOR ADJUSTMENT OR RELIEF (MAY 1994)
(Reference)
- I. 56 52.203-9 REQUIREMENT FOR CERTIFICATE OF PROCUREMENT INTEGRITY--MODIFICATION
(NOV 1990)

(a) Definitions. The definitions set forth in FAR 3.104-4 are hereby incorporated in this clause.

(b) The Contractor agrees that it will execute the certification set forth in paragraph (c) of this clause when requested by the Contracting Officer in connection with the execution of any modification of this contract.

(c) Certification. As required in paragraph (b) of this clause, the officer or employee responsible for the modification proposal shall execute the following certification:

CERTIFICATE OF PROCUREMENT INTEGRITY--MODIFICATION (NOV 1990)

(1) I, _____ [Name of certifier] am the officer or employee responsible for the preparation of this modification proposal and hereby certify that, to the best of my knowledge and belief, with the exception of any information described in this certification, I have no information concerning a violation or possible violation of subsection 27(a), (b), (d) or (f) of the Office of Federal Procurement Policy Act, as amended+ (41 U.S.C. 423), (hereinafter referred to as "the Act"), as implemented in the FAR, occurring during the conduct of this procurement _____ (contract and modification number).

(2) As required by subsection 27(e)(1)(3) of the Act, I further certify that to the best of my knowledge and belief, each officer, employee, agent, representative, and consultant of _____ [Name of Offeror] who has participated personally and substantially in the preparation or submission of this proposal has certified that he or she

is familiar with, and will comply with, the requirements of subsection 27(a) of the Act, as implemented in the FAR, and will report immediately to me any information concerning a violation or possible violation of subsections 27(a), (b), (d), or (f) of the Act, as implemented in the FAR, pertaining to this procurement.

(3) Violations or possible violations: (Continue on plain bond paper if necessary and label Certificate of Procurement Integrity--Modification (Continuation Sheet), ENTER "NONE" IF NONE EXISTS)

[Signature of the officer or employee responsible for the modification proposal and date]

[Typed name of the officer or employee responsible for the modification proposal]

- Subsections 27(a), (b), and (d) are effective on December 1, 1990.

Subsection 27(f) is effective on June 1, 1991.

THIS CERTIFICATION CONCERNS A MATTER WITHIN THE JURISDICTION OF AN AGENCY OF THE UNITED STATES AND THE MAKING OF A FALSE, FICTITIOUS, OR FRAUDULENT CERTIFICATION MAY RENDER THE MAKER SUBJECT TO PROSECUTION UNDER TITLE 18, UNITED STATES CODE, SECTION 1001.

(End of certification)

(d) In making the certification in paragraph (2) of the certificate, the officer or employee of the competing Contractor responsible for the offer or bid, may rely upon a one-time certification from each individual required to submit a certification to the competing Contractor, supplemented by periodic training. These certifications shall be obtained at the earliest possible date after an individual required to certify begins employment or association with the Contractor. If a Contractor decides to rely on a certification executed prior to the suspension of section 27 (i.e., prior to December 1, 1989), the Contractor shall ensure that an individual who has so certified is notified that section 27 has been reinstated. These certifications shall be maintained by the Contractor for a period of 6 years from the date a certifying employee's employment with the company ends or, for an agency, representative, or consultant, 6 years from the date such individual ceases to act on behalf of the Contractor.

(e) The certification required by paragraph (c) of this clause is a

material representation of fact upon which reliance will be placed in executing this modification.

(End of clause)

I.57 52.215-2 II AUDIT--NEGOTIATION (FEB 1993)--ALTERNATE II (FEB 1993)

(a) Examination of costs. If this is a cost-reimbursement, incentive, time-and-materials, labor-hour, or price-redeterminable contract, or any combination of these, the Contractor shall maintain--and the Contracting Officer or representatives of the Contracting Officer shall have the right to examine and audit--books, records, documents, and other evidence and accounting procedures and practices, regardless of form (e.g., machine readable media such as disk, tape, etc.) or type (e.g., data bases, applications software, data base management software, utilities, etc.), sufficient to reflect properly all costs claimed to have been incurred or anticipated to be incurred in performing this contract. This right of examinations shall include inspection at all reasonable times of the Contractor's plants, or parts of them, engaged in performing the contract.

(b) Cost or pricing data. If, pursuant to law, the Contractor has been required to submit cost or pricing data in connection with pricing this contract or any modification to this contract, the Contracting Officer or representatives of the Contracting Officer who are employees of the Government shall have the right to examine and audit all of the Contractor's books, records, documents, and other data regardless of form (e.g., machine readable media such as disk, tape, etc.) or type (e.g., data bases, applications software, data base management software, utilities, etc.), including computations and projections, related to proposing, negotiating, pricing, or performing the contract or modification, in order to evaluate the accuracy, completeness, and currency of the cost or pricing data. The right of examination shall extend to all documents necessary to permit adequate evaluation of the cost or pricing data submitted, along with the computations and projections used.

(c) Reports. If the Contractor is required to furnish cost, funding, or performance reports, the Contracting Officer or representatives of the Contracting Officer who are employees of the Government shall have the right to examine and audit books, records, other documents, and supporting materials, for the purpose of evaluating (1) the effectiveness of the Contractor's policies and procedures to produce data compatible with the objectives of these reports and (2) the data reported.

(c) Availability. The Contractor shall make available at its office at all reasonable times the materials described in paragraphs (a) and (b) above, for examination, audit, or reproduction, until 3 years after final payment under this contract, or for any shorter period specified in Subpart 4.7, Contractor Records Retention, of the Federal Acquisition Regulation (FAR), or for any longer period required by statute or by other clauses of this contract. In addition--

(1) If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement; and

(2) Records relating to appeals under the Disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are disposed of.

(e) Except as otherwise provided in FAR Subpart 4.7, Contractor Records Retention, the Contractor may transfer computer data in machine readable form from one reliable computer medium to another. The Contractor's computer data retention and transfer procedures shall maintain the integrity, reliability, and security of the original data. The contractor's choice of form or type of materials described in paragraphs (a), (b), and (c) of this clause affects neither the Contractor's obligations nor the Government's rights under this clause.

(f) The Contractor shall insert a clause containing all the terms of this clause, including this paragraph (f), in all subcontracts under this contract that are over the small purchase limitation in FAR Part 13, altering the clause only as necessary to identify properly the contracting parties and the Contracting Officer under the Government prime contract.

(g) The provisions of OMB Circular No. A-133 "Audits of Institutions of Higher Learning and Other Nonprofit Institutions" apply to this contract.

(End of clause)

I.58 52.242-13 BANKRUPTCY (APR 1991)

In the event the Contractor enters into proceedings relating to bankruptcy, whether voluntary or involuntary, the Contractor agrees to furnish, by certified mail, written notification of the bankruptcy to the Contracting Office responsible for administering the contract. This notification shall be furnished within five days of the initiation of the

proceedings relating to bankruptcy filing. This notification shall include the date on which the bankruptcy petition was filed, the identity of the court in which the bankruptcy petition was filed, and a listing of Government contract numbers and contracting offices for all Government contracts against which final payment has not been made. This obligation remains in effect until final payment under this contract.

(End of clause)

I.59 252.204-7003 CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992)

The Contractor's procedures for protecting against unauthorized disclosure of information shall not require Department of Defense employees or members of the Armed Forces to relinquish control of their work products, whether classified or not, to the Contractor.

(End of clause)

END OF SECTION I

SECTION J
LIST OF ATTACHMENTS

J-1. LIST OF DOCUMENTS, EXHIBITS, AND OTHER ATTACHMENTS

The following documents, exhibits, and other attachments, which are identified by Attachment Numbers in this Section J, apply to and are a part of this contract.

ATTACHMENT	TITLE	PAGES
#1	Contractor's Technical Proposal (NAS Proposal No. 94-CPSMA-154)	5
#2	Contract Security Classification Specification (DD FORM 254)	5
#3	Section 267, National Defense Authorization Act of Fiscal Year 1994	1
#4	Agreement to Establish the Allowability of Pre-Contract Costs	1

END OF SECTION J

NATIONAL ACADEMY OF SCIENCES/NATIONAL ACADEMY OF ENGINEERING
NATIONAL RESEARCH COUNCIL

Commission on Physical Sciences, Mathematics, and Applications
Computer Science and Telecommunications Board

National Cryptography Policy
(Original dated: March 1994)
(Revised dated: June 1994)

PROJECT SUMMARY

Cryptographic technologies are critical to a wide variety of important military and civilian applications involving sensitive or classified information that must be protected from unauthorized disclosure. National cryptography policy has important implications for future U.S. economic competitiveness, national security, law enforcement interests, and the protection of the rights of individual U.S. citizens. As part of the Defense Authorization Bill for FY 1994, the Secretary of Defense is asked to request from the National Research Council (NRC) a comprehensive study on cryptographic technologies and national cryptography policy. This study is expected to address the appropriate policy balance among the various interests described above (with a particular focus on how technology affects the policy options for balancing these interests), the strength of various cryptographic technologies known today and anticipated in the future that are relevant for commercial purposes; and possible strengths and shortcomings in the federal process through which national cryptography policy has in fact been formulated, as well as recommendations for improving national cryptographic policy in the future. A study committee of approximately 16 members will include expertise in computer and communications technology; cryptographic technologies and cryptanalysis; foreign, national security, and intelligence affairs; law enforcement; science policy; trade policy; commercial and business dimensions of computer technology (hardware and software vendors, users of cryptographic technologies); and interests in privacy and civil liberties. Nominations for the committee will be sought from relevant NRC oversight boards; members of IOM, NAS, and NAE; and other experts.

ORIGIN AND BACKGROUND

Cryptographic technologies are critical to a wide variety of important military and civilian applications involving sensitive or classified information that must be protected from unauthorized disclosure. In addition, cryptography is a key component of most authentication technologies, i.e., technologies to guarantee the identity of a message's sender. National cryptography policy has important implications for future U.S. economic competitiveness, national security, and law enforcement interests. It also bears on the protection of the rights of private U.S. citizens.

Cryptography policy has historically been dominated by national security considerations, reflecting the U.S. government's needs for effective cryptographic protection of classified and other sensitive communications as well as its needs to gather intelligence for national security purposes, needs that would benefit from U.S. superiority in cryptographic technologies. National security concerns have motivated such actions as development of cryptographic technologies, development of countermeasures

to reverse the effects of encryption, and review and approval of cryptographic technologies for export. Although cryptography does and will remain important to national security, it has attracted broader interest, and national security is no longer the sole policy driver for this class of technology.

A major development in the past ten years has been what could be called the popularization of cryptography. First, some industries--notably financial services--have come to rely on encryption as an enabler of secure electronic funds transfers. Second, other industries have developed an interest in encryption for protection of proprietary and other sensitive information. Third, the broadening use of computers and computer networks has generalized the demand for technologies to secure communications down to the level of individual citizens and assure the privacy and security of their electronic records and transmissions. Fourth, the sharply increased use of wireless communications (e.g., cellular telephones) has highlighted the higher vulnerability of such communications to unauthorized intercept as well as the impossibility of detecting these intercepts.

These trends have been associated with efforts to develop civilian or commercial encryption systems and to integrate cryptographic technologies with other products (such as communications systems or computer software). Many products that incorporate cryptographic technologies are available in the United States and abroad. These phenomena have created commercial interests in the market for cryptographic technologies and systems incorporating such technologies--a competitiveness concern--as well as heightened debate over individual need for and access to technologies to protect individual privacy.

Still another consequence of the expectation of widespread use of encryption is the emergence of law enforcement concerns that parallel, on a civilian basis, some of the national security concerns. Law enforcement officials fear that wide dissemination of effective cryptographic technologies will impede their efforts to collect information necessary for pursuing criminal investigations. On the other side, civil libertarians fear that controls on cryptographic technologies will give government authorities unprecedented and unwarranted capabilities for intrusion into the private lives of citizens.

Attempting to balance these concerns, the Clinton Administration proposed on April 16, 1993, the use of a particular cryptographic technology--an encryption chip to be implemented with a so-called "key-escrow" system--that could be used to ensure the privacy of voice communications but still enable law enforcement authorities to listen to such conversations pursuant to court order. The system proposed is based on an electronic microcircuit originally known as the Clipper Chip and two restricted-access databases that would hold the cryptographic keys necessary to decode communications encrypted by the Clipper Chip. Access to these databases would, in principle, be permissible only through court order.

A letter report on the proposed system authored by the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC) was transmitted to the White House on June 11, 1993. This report noted that the issues raised by the proposed system were part of a larger question regarding the nature and status of national cryptography policy, and noted that the CSTB would be both willing and able to conduct an impartial and independent study of this policy.

As part of the Defense Authorization Bill for FY 1994, the Secretary of Defense is asked to request a comprehensive study from the National Research Council on cryptographic technologies and national cryptography policy.

PROPOSED ACTIVITY

Project Content

It is expected that the study will address:

- the impact of current and possible future restrictions on and standards for cryptographic technology on
 - + the availability of such technology to foreign and domestic parties with interests hostile to or competitive with the national security, economic, commercial, and privacy interests of the U.S. government, U.S. industry, and private U.S. citizens.
 - + the competitiveness of U.S. manufacturers of such technology in the international market.
 - + the competitiveness and performance of commercial U.S. users of such technology.
 - + U.S. national security and law enforcement interests:
- the strength of various cryptographic technologies known today and anticipated in the future that are relevant for commercial and private purposes;
- current and anticipated demand for information systems security based on cryptography;
- the impact of foreign restrictions on the use of, importation of, and the market for cryptographic technology;
- the extent to which current cryptography policy is adequate for protecting U.S. interests in privacy, public safety, national security, and economic competitiveness;
- technical strengths and weaknesses of current key escrow implementation schemes;
- how technology now and in the future affects and will affect the feasible policy options for balancing the national security and law enforcement interests of government and the privacy and commercial interests of U.S. industry and private U.S. citizens;
- recommendations for the process through which national security, law enforcement, commercial, and privacy interests are balanced in the formulation of national cryptography policy.

Project Structure

CSTB will assemble a committee of approximately 16 members that will include expertise in computer and communications technology; cryptographic technologies and cryptanalysis; foreign, national security, and intelligence affairs; law enforcement; science policy; trade policy; commercial and business dimensions of computer technology (hardware and software vendors, users of cryptographic technologies); and interests in privacy and civil liberties. Nominations for the committee will be sought from relevant oversight boards; members of IOM, NAS, and NAE; and other experts.

To complete the study, the project plan calls for six three-day meetings of the full committee and other meetings of sub-committees as appropriate.

It is expected that this study will require the handling of sensitive and highly classified information; extra time and staff effort has been planned to accommodate this fact. A subpanel of the full committee will be cleared at the SI/TK level and have access to all relevant information to ensure that the findings, conclusions, and recommendations of the unclassified report are consistent with what is known in the classified world. Access to classified data is understood to be contingent on the successful completion of required background checks and investigations on committee members and staff and the execution of non-disclosure agreements by those individuals.

The National Academy of Sciences has prepared and maintains a Standard Practice Procedures (SPP) Manual that implements the requirements of the DoD Industrial Security Manual (ISM). The SPP manual has been reviewed and approved by the Defense Investigative Service. The study will conform to all requirements and procedures specified in the SPP manual related to classified information.

The project plan calls for the following steps in report preparation. After the committee has completed its deliberations, a draft report will be prepared and revised in accordance with committee direction. This draft report will be submitted internally within the NRC for review (see below). After the report clears the NRC review process, it will be edited internally for organization, consistency, and clarity. After NRC editing, which is a major step in the report preparation process, the report will be ready for transmittal to the Defense Department for security review. All necessary redactions will be made to the report by the NRC, after which the report will be transmitted to the Secretary of Defense and dissemination activities will begin as described below.

PRODUCT AND DISSEMINATION PLAN

In accordance with Public Law 103-160, the Defense Authorization Bill for Fiscal Year 1994, the project plan calls for the study will be delivered to the Secretary of Defense approximately two years after full processing of all necessary security clearances. However, the NRC will make every attempt to deliver the study sooner, and it currently believes that the core work of the study will be completed about 18 to 20 months after execution of the award instrument for funding the study.

The final report of the study committee would be subject to NRC review procedures. It is the intent of the project to submit the report to the Defense Department in unclassified form, with classified annexes as necessary. The NRC review procedures will ensure that only individuals with appropriate security clearances will be selected as reviewers for the classified annexes, should such annexes be necessary.

The report will be submitted to the Department of Defense prior to publication in final form for security review to ensure that classified material is not inadvertently disclosed. The governing statute provides that 120 days after the day on which the report is submitted to the Secretary of Defense, the Secretary shall submit the report to the Committees on Armed Services, Intelligence, Commerce, and the Judiciary of the Senate and House of Representatives in unclassified form, with classified annexes as necessary.

It is expected that when the Secretary submits the report to Congress, the NRC would hold a press conference to discuss the unclassified version of the report. In accordance with the Academy's broad charge to disseminate its work widely so as to promote a more informed public discussion of the issues,

the NRC will also publish the unclassified version of the report and conduct briefings and discussions for several months following the initial public release of the report. Such dissemination efforts are typical for all major NRC reports.

REPORTS

Presidential Executive Order 12832 of January 19, 1993 amends Executive Order 2859, which established the National Research Council (NRC) reaffirming and clarifying the NRC's relationship with the U.S. Government. Of particular relevance to this proposal, the Executive Order directs the NRC to disseminate to duly accredited persons and the public the scientific and technical information it gathers and collates. Further, the actual expense of such report shall be paid to the Academy through grants-in-aid and contracts by executive departments and agencies. The Academy's acceptance of an award by a department or agency of the U.S. Government, is conditioned upon adherence to the letter and spirit of the Executive Order which provides the framework within which the NRC and the Government are expected to interact. The Government printing and binding regulations intend that contractors do not become prime or substantial sources of printing for departments or agencies. The Executive Order requirement that the NRC disseminate its reports is interpreted as not being primarily or substantially for the purpose of having such findings printed for the use of a department or agency and therefore outside the limitations of the printing and binding regulations. Accordingly, included in the attached estimate of costs is an amount projected to cover the cost of reproducing reports for this activity.

EXPENDITURES AND SOURCES OF FUNDS

The estimated cost of this thirty-two month activity is \$798,735, which is being requested from the Department of Defense.

CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

a. FACILITY CLEARANCE REQUIRED

TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED

SECRET

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		3. THIS SPECIFICATION IS: (X and complete as applicable)	
<input checked="" type="checkbox"/> a. PRIME CONTRACT NUMBER DASW01-94-C-0178		<input checked="" type="checkbox"/> a. ORIGINAL (Complete date in all cases)	Date (YYMMDD) 940929
b. SUBCONTRACT NUMBER		b. REVISED (Supersedes all previous specs)	Revision No. Date (YYMMDD)
c. SOLICITATION OR OTHER NUMBER	Due Date (YYMMDD)	c. FINAL (Complete Item 6 in all cases)	Date (YYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT? YES NO. If Yes, complete the following:
 Classified material received or generated under (Preceding Contract Number) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 2547 YES NO. If Yes, complete the following:
 In response to the contractor's request dated , retention of the identified classified material is authorized for the period of

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE National Academy of Sciences P. O. Box 57062- West End Station Washington, DC 20037	b. CAGE CODE 5B946	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DIS, Director of Industrial Security 25 South Quaker Lane Room 23 Alexandria, VA 22314
---	-----------------------	---

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
--------------------------------	--------------	--

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
-------------	--------------	--

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

In connection with the 1994 Defense Authorization Act, the National Academy of Sciences' Computer Science and Telecommunications Board will undertake a Congressionally Mandated Study entitled Comprehensive Independent Study of National Cryptography Policy

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input type="checkbox"/>
b. RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input type="checkbox"/>
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY	<input type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/>
(2) Non-SCI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	<input checked="" type="checkbox"/>
g. NATO INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS	<input type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER (Specify)	<input type="checkbox"/>
k. OTHER (Specify)	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

Direct

Through (Specify):

The individual identified in Block 16.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
 *In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

See attached continuation sheets.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) Yes No

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.) Yes No

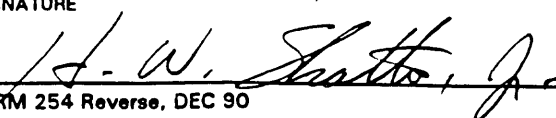
16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL H. W. SHATTO, JR.	b. TITLE Contracting Officer	c. TELEPHONE (Include Area Code) (703) 614-4579
---	-------------------------------------	--

d. ADDRESS (Include Zip Code)
 Defense Supply Service-Washington
 5200 Army Pentagon
 Washington, DC 20310-5200

17. REQUIRED DISTRIBUTION

<input checked="" type="checkbox"/>	a. CONTRACTOR
<input type="checkbox"/>	b. SUBCONTRACTOR
<input checked="" type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
<input type="checkbox"/>	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
<input checked="" type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input type="checkbox"/>	f. OTHERS AS NECESSARY

e. SIGNATURE


Use and designation of Type C Consultants in accordance with paragraph 2-111c, Industrial Security Manual for Safeguarding Classified Information (ISM), DoD 5220.22-M, is authorized under this Contract.

10a. Communications Security (COMSEC) Information. Secure Telephone Unit (STU) STU III only COMSEC Account is necessary. Access to classified COMSEC information requires a special briefing and a final U.S. Government clearance at the appropriate level.

10e. INTELLIGENCE INFORMATION: Sensitive Compartmented Information (SCI). The Cognizant Security Office (CSO) identified in Block 6c is relieved of inspection responsibility for SCI, but is responsible for inspections of non-SCI in the possession of the prime contractor. Access to intelligence information requires a final U.S. Government clearance at the appropriate level.

This contract requires access to SCI. The CNR SSO (Mrs. Jane Klug) has exclusive responsibility for all SCI material released to or developed under this contract. Access to SCI is limited to that at a U.S. Government SCIF or other contractor SCIF. DIAM 50-5 and DoD 5105 series provides the necessary guidance. No contractor personnel will be granted access to SCI material under this contract unless they are filling an SCI billet. The contractor will coordinate with the SCI Contract Monitor to ensure adequate billets are requested under this contract. Multiple contract participants sponsored by organizations other than CNR SSO must be permanently certified to the CNR SSO for use on this contract. The contractor will designate a Special Security Point of Contact (POC) to the CNR SSO. The POC will be responsible for all personnel and information security transactions between the contractor and CNR SSO. The security classification guides for SCI are DoD TS-5105.21-M2+M3 and DoD TS-5005.21-M-3. The contractor must restrict access to all classified information only to those individuals who possess the necessary security clearance and who are actually providing services under this contract. Further dissemination of SCI to other contractors, subcontractors, or other government agencies, private individuals or organizations, is prohibited unless authorized in writing from the releasing agency.

- These supplementary requirements will be provided to the Contractor by the CNR SSO.
- SCI support of this contract is under the exclusive responsibility of the designated SSO and will be identified to the appropriate DIS Security Office by the Special Security Point of Contact.

CONTINUATION SHEET 02 of 03, DD FORM 254

issued under Contract No. DASW01-94-C-0178

- SCI will not be released to any activity or person of the contractor's organization not directly engaged in providing services under the contract, or to another contractor (including subcontractors), government agency, private individual, or organization without specific release approval of the originator of the material, as outlined in governing directive, and prior approval and certification of "need-to-know" by contract monitor.
- SCI will not be released to foreign nationals or immigrant aliens who may be employed by the contractor, regardless of the level of their security clearance.
- Names of contractor personnel requiring access to SCI will be submitted to the CNR SSO for approval. CNR SSO will submit request(s) for Single Scope Background Investigations in accordance with the Industrial Security Manual.
- SCI data and material will be stored and maintained only in properly accredited facilities. Under no circumstances will SCI be furnished to the contractor's facility.
- Inquiries pertaining to classification guidance regarding SCI will be directed to the CNR SSO.
- The contractor will not use references to SCI access, even by unclassified acronyms, in advertising, promotional efforts, or recruitment for employees.

INTELLIGENCE INFORMATION SHEET

- Intelligence information does not become the property of the contractor and may be withdrawn at any time. Upon expiration of the contract, all intelligence released and any material using data from the intelligence will be returned to the contracting officer for security matters, or authorized representative for final disposition. Only with prior authorization may the contractor retain such material.
- The prime contractor will not release the intelligence material to any activity or person of the contractor's organization not directly engaged in providing services under the contract or to another contractor (including subcontractors), government agency, private individual, or organization without prior approval.
- Intelligence material will not be released to foreign national or immigrant aliens who may be employed by the contractor, regardless of the level of their security clearance.
- Intelligence material will not be reproduced without prior approval.

CONTINUATION SHEET 03 of 03. DD FORM 254

issued under Contract No. DASW01-94-C-0178

- The prime contractor will maintain records which will permit them to furnish, on demand, the names of individuals who have had access to intelligence material in their custody.

10j. For Official Use Only Information (FOUO). The *"For Official Use Only"* Information provided under this contract shall be safeguarded as specified in Chapter 13, Section 6, ISM.

11c. Receive and generate classified material. Classification and regrading/declassification markings of documentation produced by the prime contractor and/or Type C Consultants will be consistent with that applied to the information or documentation from which the new document was prepared. If a compilation of the information or a complete analysis of a subject appears to require a security classification other than that of the source documentation, the material will be assigned the tentative security classification and request instructions from the office shown in item 16a. Pending final determination, the material will be safeguarded as required for its assigned or proposed classification whichever is higher, until classification is changed or otherwise verified.

Only those contractor employees requiring access to classified information in the performance of this contract shall be granted security clearances under the Industrial Security Program.

11g. Be authorized to use the services of DTIC or other secondary distribution center. The DD Form 1540 and DD Form 1541 will remain active and be kept up-to-date by the contractor for the duration of this contract.

11h. Require a COMSEC Account. A STU-III only Account will be maintained by the contractor.

SEC. 267. COMPREHENSIVE INDEPENDENT STUDY OF NATIONAL CRYPTOGRAPHY POLICY.

(a) **STUDY BY NATIONAL RESEARCH COUNCIL.**—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall request the National Research Council of the National Academy of Sciences to conduct a comprehensive study of cryptographic technologies and national cryptography policy.

(b) **MATTERS TO BE ASSESSED IN STUDY.**—The study shall assess—

(1) the effect of cryptographic technologies on—

(A) national security interests of the United States Government;

(B) law enforcement interests of the United States Government;

(C) commercial interests of United States industry; and

(D) privacy interests of United States citizens; and

(2) the effect on commercial interests of United States industry of export controls on cryptographic technologies.

(c) **INTERAGENCY COOPERATION WITH STUDY.**—The Secretary of Defense shall direct the National Security Agency, the Advanced Research Projects Agency, and other appropriate agencies of the Department of Defense to cooperate fully with the National Research Council in its activities in carrying out the study under this section. The Secretary shall request all other appropriate Federal departments and agencies to provide similar cooperation to the National Research Council.

(d) **FUNDING.**—Of the amount authorized to be appropriated in section 201 for Defense-wide activities, \$300,000 shall be available for the study under this section.

(e) **REPORT.**—(1) The National Research Council shall complete the study and submit to the Secretary of Defense a report on the study within approximately two years after full processing of security clearances under subsection (f). The report on the study shall set forth the Council's findings and conclusions and the recommendations of the Council for improvements in cryptography policy and procedures.

(2) The Secretary shall submit the report to the Committee on Armed Services, the Committee on the Judiciary, and the Select Committee on Intelligence of the Senate and to the Committee on Armed Services, the Committee on the Judiciary, and the Permanent Select Committee on Intelligence of the House of Representatives not later than 120 days after the day on which the report is submitted to the Secretary. The report shall be submitted to those committees in unclassified form, with classified annexes as necessary.

(f) **EXPEDITED PROCESSING OF SECURITY CLEARANCES FOR STUDY.**—For the purpose of facilitating the commencement of the study under this section, the Secretary of Defense shall expedite to the fullest degree possible the processing of security clearances that are necessary for the National Research Council to conduct the study.



REPLY TO
ATTENTION OF

ATTACHMENT #4
(DASW01-94-C-0178)

Page 1 of 1

ACQUISITION DIRECTORATE
JDSS-W/AR2/HWS

AGREEMENT TO ESTABLISH THE ALLOWABILITY OF
PRE-CONTRACT COSTS
DASW01-94-R-0224

WHEREAS, a valid and properly funded requirement exists to provide support to the Office of the Assistant Secretary of Defense, Director of Information Systems Security entitled "NATIONAL CRYPTOGRAPHY POLICY."

WHEREAS, the proposed contractor, National Academy of Sciences (NAS), has agreed to perform work in general accordance with the Statement of Work (SOW) revised dated 20 June 1994;

WHEREAS, the government and NAS will negotiate in good faith to reach contractual agreement; and

WHEREAS, the Government requires immediate support;

NOW, THEREFORE, in accordance with FAR 31.205-32, the following agreements are made pursuant to the requirements of FAR 31.109.

FIRST: In the event that a contract is awarded, precontract costs not to exceed \$50,000.00 shall be an allowable expense provided that the individual cost be incurred no sooner than 21 July 1994 and no precontract costs shall be allowable if incurred after 30 September 1994 unless further written agreement is made.

SECOND: It is understood by both parties that any costs incurred prior to final agreement on the proposed contract are incurred voluntarily on the part of the contractor and at his/her own risk.

The undersigned acknowledge the aforementioned agreements.

Date: 16 September 1994

Name: Robert R. Kelley
Title: Manager of Federal Contract

CONCUR:

Date: SEP 16 1994

H.W. SHATTO
Contracting Officer