The original documents are located in Box C54, folder "Presidential Handwriting, 1/12/1977" of the Presidential Handwriting File at the Gerald R. Ford Presidential Library.

THE WHITE HOUSE

WASHINGTON

January 12, 1977

MR PRESIDENT:

Securing U.S. Telecommunications

The attached memorandum prepared by Brent Scowcroft and Jim Cannon was reviewed by Jack Marsh and Phil Buchen. They commented as follows:

Phil Buchen (Ed Schmults): "We concur in the NSC and Domestic Council recommendations and wish to stress the importance, in the Counsel's office view, of the need to carefully explain the program to the Congress and the American public so that it will not be seen as a threat by military-intelligence communities to the privacy of the public's communications network."

Jack Marsh: "Rather than include this in the State of the Union, I recommend this be a subject the President discuss personally or refer by memo to the President-elect."

Jim Connor

Original package returned to 718 C 1/12/77

Mr. Marsh borrowed the package on 1/14/77

ITEM WITHDRAWAL SHEET
WITHDRAWAL ID 01042

Collection/Series/Folder ID No.	:	004700174
Reason for Withdrawal	:	NS,National security restriction
Type of Material	:	MEM,Memo(s)
Creator's Name	:	Brent Scowcroft and Jim Cannon
Receiver's Name	:	President
Description	:	re telecommunications
Creation Date	:	01/06/1977
Volume (pages)	:	1
Date Withdrawn	:	05/25/1988

January 12, 1977

MR PRESIDENT:

Securing U.S. Telecommunications

The attached memorandum prepared by Brent Scowcroft and Jim Cannon was reviewed by Jack Marsh and Phil Buchen. They commented as follows:

Phil Buchen (Ed Schmults): "We concur in the NSC and Domestic Council recommendations and wish to stress the importance, in the Counsel's office view, of the need to carefully explain the program to the Congress and the American public so that it will not be seen as a threat by military-intelligence communities to the privacy of the public's communications network."

Jack Marsh: "Rather than include this in the State of the Union, I recommend this be a subject the President discuss personally or refer by memo to the President-elect."

Jim Connor

THE WHITE HOUSE

ACTION MEMORANDUM WASHINGTON LOG NO.:

Date: January 6, 1977 Time:

FOR ACTION: cc (for information):

Jack Marsh
✓ Phil Buchen

FROM THE STAFF SECRETARY

DUE: Date: Friday, January 7 Time: 10 AM

SUBJECT:

Joint Memorandum from Brent Scowcroft and
Jim Cannon re Securing U.S. Telecommunications
dated 1/6/77

ACTION REQUESTED:

____ For Necessary Action ___X For Your Recommendations

____ Prepare Agenda and Brief ____ Draft Reply

__X__ For Your Comments ____ Draft Remarks

REMARKS:

Your quick response is request as this might be
something to be added to the State of the Union.

Buchen - see comments

// Top Secret //

UNCLASSIFIED UPON REMOVAL
OF CLASSIFIED ATTACHMENTS

PLEASE ATTACH THIS COPY TO MATERIAL SUBMITTED.

If you have any questions or if you anticipate a delay in submitting the required material, please telephone the Staff Secretary immediately.

Jim Connor
For the President

THE WHITE HOUSE

WASHINGTON

January 7, 1977

MEMORANDUM FOR: JIM CONNOR

FROM: ED SCHMULTS

SUBJECT: Joint Memorandum from Brent Scowcroft and Jim Cannon re Securing U.S. Telecommunications dated 1/6/77

We concur in the NSC and Domestic Council recommendations and wish to stress the importance, in the Counsel's office view, of the need to carefully explain the program to the Congress and the American public so that it will not be seen as a threat by military-intelligence communities to the privacy of the public's communications network.

cc: Philip Buchen

[redacted]

THE WHITE HOUSE

A[redacted]ORANDUM

WASHINGTON

~~Top Secret~~

LOG NO.:

D[redacted]January 6, 1977

Time:

FOR ACTION:

cc (for information):

Jack Marsh
Phil Buchen

FROM THE STAFF SECRETARY

DUE: Date: Friday, January 7 Time: 10 AM

SUBJECT:

Joint Memorandum from Brent Scowcroft and
Jim Cannon re Securing U.S. Telecommunications
dated 1/6/77

ACTION REQUESTED:

____ For Necessary Action

____ Prepare Agenda and Brief

__X__ For Your Comments

__X__ For Your Recommendations

____ Draft Reply

____ Draft Remarks

REMARKS:

Your quick response is request as this might be
something to be added to the State of the Union.

January 12

Rather than include this in the State of the Union, I recommend this be a subject the President discuss personally or refer by memo to the President-elect.

Jack Marsh

~~Top Secret~~

UNCLASSIFIED UPON REMOVAL
OF CLASSIFIED ATTACHMENTS

PLEASE ATTACH THIS COPY TO MATERIAL SUBMITTED.

If you have any questions or if you anticipate a delay in submitting the required material, please telephone the Staff Secretary immediately.

Jim Connor
For the President

MEMORANDUM

6726-X

THE WHITE HOUSE

WASHINGTON

~~TOP SECRET~~ - XGDS (2)

ACTION

January 6, 1977

MEMORANDUM FOR: THE PRESIDENT

FROM: BRENT SCOWCROFT
JIM CANNON

SUBJECT: Securing U.S. Telecommunications

Background

Your earlier decision on securing U.S. telecommunications included immediate steps to reduce the opportunities for Soviet communications intercept by moving government and defense contractor circuits from microwave to less vulnerable cable. However, the limited availability of cable and its exclusive control by a single common carrier impose the need for other means in achieving wider protection. These earlier decisions also directed development of technologies for wide-scale protection of microwave circuits, as well as preparation of implementation plans to achieve broad protection of both government and private sector communications.

The next major step is to decide whether or not to proceed at this time with wide-scale protection of the domestic telecommunications system. A decision to do so would require public explanation of the vulnerability of our communications network. In reaching a decision on total protection, two recently completed studies -- an intelligence community damage assessment and a review of our technical readiness to proceed -- provide valuable background data.

Damage Assessment

The intelligence community assessment of the damage resulting from Soviet intercept options (Tab A) confirms our earlier concerns and provides specific examples of damage to national interests resulting from Soviet intercept of private sector as well as defense contractor communications. [redacted]

~~TOP SECRET~~ - XGDS

[redacted] the circumstantial evidence makes a convincing case for extending protection to private sector communications on a broad scale.

Technology Assessment

An NSC technical advisory panel recently reviewed the status of the technology to determine if there were any major technical uncertainties or risks in proceeding with wide-scale protection of the domestic telecommunications network (Tab B). The Panel concluded that the technology program is sufficiently broad and the technical risks are sufficiently manageable that there is no technical reason to defer a decision to proceed. The Panel further pointed out that no single technology will provide a permanent solution to the telecommunications security problem. An evolutionary approach, involving successive application of a number of technologies, will be required, with the pace being set by Soviet advances in breaking our protection system and by the evolution of our domestic telecommunications system.

Decisions

There are two basic decisions that can be made at this time: whether to proceed with the protection of the private sector telecommunications, and whether to explain publicly the vulnerability of our telecommunications system and the need for protection.

Protection of the Private Sector

There are several advantages in moving ahead now with communications protection in the private sector:

- Such action would place further emphasis on the communications security problem, helping to assure that it receives continuing and timely attention by the next Administration.

- The damage to the national interests resulting from continuing intercept of private sector communications is great. Broad-scale remedial actions need to be implemented as soon as possible.

- The possibility of public disclosure of the problem without corresponding government action would likely result in disorganized responses by the telecommunications carriers and private sector users which could be disruptive to the domestic communications network and may not, in fact, substantially improve communications security.

The main problem, from a foreign intelligence perspective, in moving ahead with communications protection is that is may stimulate the Soviets to take even greater protective measures for their own telecommunications and thereby deny us a valuable and possibly irreplaceable source of information. However, a Presidential decision to knowingly permit the Soviets to listen to private telecommunications in the U.S. -- when there is a technical means to halt it -- in order to possibly preserve an external intelligence source would be highly criticized if such a decision became known. In addition there is an alternate view that the pace of the Soviet program to protect their communications is set by their recognition of the vulnerability of those communications and is relatively unaffected by U.S. communications security actions.

A secondary disadvantage of proceeding with the protection of the private sector is that some of the smaller common carriers, which depend almost entirely on microwave transmission, are currently suffering cash flow and capital problems. The cost of adding protective equipment, though not a major outlay and recoverable at least in part from user charges, could put these carrier at a competitive disadvantage relative to the larger common carriers.

Public Explanation

There are several reasons for making a public explanation of the vulnerability of the domestic telecommunications network and (possibly) the Soviet intercept problem at this time:

- Public explanation will alert private sector institutions to the potential damage from uncontrolled use of the telephone, allowing implementation of administrative procedures to reduce losses.

- Public explanation would place the actions of this Administration in the proper prospective. It is particularly important for the Government to create a favorable climate for public acceptance of communications security so that it is correctly perceived as a means to increased privacy and not as a threat to individual civil rights. Ongoing GAO investigations of the vulnerability of the telephone system to intercept and wiretap, the continuing activities of the House Government Information and Individual Rights Sub-committee staff in investigation of alleged government invasion of privacy, and possible inadvertent disclosure during transition might distort government actions, making them appear as an extension of the military/intelligence organizations.

- Even though some of the technologies will not be ready for application for a year or more, it will be necessary for many more people in both government and the private sector to become aware of the vulnerability problem within the next few months if planning and implementation of approved protection measures are to proceed without delay. For example, in the memorandum at Tab C, the Secretary of Defense proposes to inform all defense contractors of the intercept threat. Public explanation would facilitate dealing with the defense community, the commercial telecommunications carriers and the critical private sector institutions on this problem.

- Public explanation will place emphasis on this important problem and will assure that it receives continuing attention by the next Administration.

The disadvantages of public explanation are:

- It forewarns the Soviets, possibly increasing the sophistication of their efforts and making it more difficult to successfully counter their operations.

- It could be an additional stimulus for Soviet countermeasures against our own monitoring of their communications.

- It could trigger a strong, public anti-Soviet reaction.

- It could create demands for immediate remedial actions which are beyond current technical capabilities.

In the event of an affirmative decision, a public explanation could make the following points:

- The growth of microwave radio in our long-distance telephone system has greatly increased its vulnerability to foreign or domestic intercept.

- Microwaves are open and anyone with the proper equipment in the right location can intercept and record communications.

- Inexpensive and unobtrusive means for intercept are readily available on the commercial market and can be used by other foreign countries, organized crime, industrial espionage agents, or other unscrupulous domestic elements to eavesdrop on telephone conversations. [As an additional option, it could be stated that a foreign power is conducting telephone interception in certain localities.]

- Such actions are an invasion of individual privacy, are detrimental to national interests, and are a threat to national security.

- This has been a problem of real concern to your Administration, which has undertaken a major program to improve the security of communications:

  -- Special technologies are being developed for long-term, wide-scale, low-cost protection of the domestic communications network.

  -- In the interim, short-term steps have been taken to protect critical government and national security information.

- Continuing attention to improvement in telecommunications security will be an important problem for the new Administration. In the interim, care should be exercised in uses of these communications.

Implementation Alternatives

A long-range plan has been prepared for wide-scale application of communications protection in the domestic communications network, first in Washington, New York, and San Francisco areas, and eventually

nationwide. This plan (a summary is at Tab D) provides for protection of all communications in these areas, both private and government, including protection of satellite communications as well as the terrestrial microwave network. Two major alternatives for the government/industry role are considered:

- The first alternative would minimize the government role through a cooperative government/industry effort. Required use of approved commercially-provided, secure communication services by government agencies and defense contractors would be expected to create a market demand for secure communications as well as providing needed improvements in security. These market forces, working in conjunction with a government-sponsored educational campaign to increase public awareness of the intercept threat, would be expected to provide the incentive for broad application of communications security. The drawback to this alternative is the lack of certainty that such broad protection would in fact materialize.

- The second alternative is surer but would require stronger government action to meet the threat through a Federally-mandated program directing implementation of approved protection techniques throughout the national microwave network. This approach would require implementing legislation and might well require the government to make sensitive choices as to which sectors of the private sector would be protected and which would not.

In either alternative, the government would need to establish policy, standards and regulations, would assist the private sector by making government-developed crypotgraphic technology available for commercial application, and would promote public acceptance of the need for communications security by making the private sector aware of the nature and scope of the threat. Industry would apply bulk protection techniques to the communications networks and would pass the added costs to the users. The total cost of protecting the Washington, New York and San Francisco areas is estimated to be $200-300 million, corresponding to less than a one percent increase in the telephone rate base. The cost of nationwide protection is estimated to be $1.0-2.0 billion.

The decision on which of the two alternative approaches to implementing protection cannot appropriately be made at this time. Consultations need to be carried out with the communications industry, key members of Congress, and the FCC before making a final decision.

Organizational Considerations

Since telecommunications security for the United States is a problem without precedent, no existing government entity is structured to deal with it on a permanent basis. This will be an important organizational issue for the new Administration. If you wish to move forward with the program now, a directive could be issued to establish a new organization on telecommunications security, possibly chaired by the Vice President.

A study has been recently completed by the NSC, Domestic Council, OMB, and OTP which considered a number of options for continuing oversight of the communication security problem (Tab E). Basically, the options are two-fold: either to vest a single agency with the mandate to implement a national telecommunication security program, or to deal with the problem on an interagency basis involving a continuing White House management role.

- The first alternative has the advantage of avoiding management by committee, and could be effective if the agency head accepted this program as a priority matter. The main disadvantage of selecting a single agency is that the obvious agency -- the one with the expertise in encryption -- is the Defense Department. It might be difficult to obtain Congressional support for having DOD involved in private sector telecommunications, both from the point of view that the defense/intelligence community does not belong in this area, and that DOD would not be sensitive to the business/commercial problems of the common carriers.

- A White House committee would assure continuing high priority to the implementation of the protection of private sector telecommunications, and by involving the domestic as well as national security interests, the objections mentioned above would be mitigated. Much of the programmatic work would still be carried out by DOD, but the interfaces with the communications industry, Congress, and the FCC would be through the committee.

Our discussions with the Vice President, who has been personally concerned for some time about the interception of U.S. telecommunications, support the concept of a joint committee being established by the National Security Council and the Domestic Council to take the lead in protecting telecommunications.

RECOMMENDATIONS

That you approve proceeding with a program to protect the private sector as well as government communications.

a. Approve_____

b. Disapprove (defer the decision)_____

2. That you approve the public explanation of the vulnerability of U.S. telecommunications, possibly as part of the State of the Union address.

a. Approve_____

b. No public announcement at this time_____

3. That you approve the establishment of a joint National Security Council/Domestic Council Committee on Telecommunications Security to oversee this effort.

a. Approve_____

b. Approve, and chaired by the Vice President_____

c. Alternatively, direct the Secretary of Defense to take the responsibility_____

d. Disapprove (defer the organizational decision)_____

A

ITEM WITHDRAWAL SHEET
WITHDRAWAL ID 01044

Collection/Series/Folder ID No.	:	004700174
Reason for Withdrawal	:	NS,National security restriction
Type of Material	:	REP,Report(s)
Description	:	re intelligence matters
Creation Date	:	10/21/1976
Volume (pages)	:	29
Date Withdrawn	:	05/25/1988

B

01045

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

December 17, 1976

~~TOP SECRET~~ (XGDS)

Dear General Scowcroft:

Recently, the special NSC Telecommunications Security Advisory Panel reviewed the status of the NSA technology program for bulk protection of microwave communications. The purpose of this review was to determine if the technology had progressed to the point that a decision could be made to proceed with protection of the Washington, New York, and San Francisco areas. The Panel included the participation of NSA, DTACCS, DCA and OTP as well as several independent consultants to the NSC.

The NSA program for development of bulk microwave protection techniques includes the following major elements:

-- Spreading. A low cost technique for frequency scrambling which can rapidly be applied to all channels of a microwave link to achieve a moderate level of protection.

-- Smearing. A more sophisticated and more expensive technique for phase scrambling of voice messages which can be added to spreading to achieve a higher level of protection.

-- TES. A more sophisticated and more expensive technique for time element scrambling which either alone, or in conjunction with spreading will provide a higher level of protection.

-- Digital Encryption. A technique which potentially provides the highest level of protection and can be readily applied to digital data traffic, but requires expensive and difficult high speed analog/digital conversion if it is to be used with voice traffic.

-- Others. Other technologies include key generator developments to support all of the above techniques, and development

XGDS of E. O. 11652 by authority of Brent Scowcroft; Exemption Category Section 5(B)(2).

of interfaces with common channel interoffice signaling (CCIS), a technique being used by AT&T in their new electronic switching centers to separate the signaling traffic from the message traffic.

Following this review, the Panel reached the following conclusions:

1. The Panel restates its view that no single technology will provide a permanent solution to the telecommunications security problem. Securing critical U.S. telecommunications will require an evolutionary approach involving successive application of a number of evolving technologies with the pace set by Soviet advances and by the evolution and growth of our domestic telecommunications system.

2. The Panel believes that early experimental test of spreading technology on the Wash 1 link will resolve a number of operational issues and should proceed at the earliest date. The Panel strongly endorses the current plan to start test transmissions by October 1977.

3. The Panel believes that the NSA technology program is sufficiently broad and the technical risks are sufficiently understood that the decision to proceed with protection of microwave communications in the three PCZ's can be made now, and need not wait for the results of the initial tests on the Wash 1 link.

4. The Panel believes that spreading will seriously impede Soviet intercept operations. It is the Panel's judgment that the benefits of spreading are sufficiently great; i.e., the opportunity to provide some protection to all communications in a given area in a short time at low cost, that spreading should be implemented in the PCZ's at the earliest possible date. However, the time period over which this technology will be fully effective against the Soviet threat is uncertain--perhaps as short as one year. Therefore, the Panel believes that an appropriate mix of techniques for augmenting spreading such as TES, smearing, and other elements in the library of comsec techniques currently being developed by NSA must be implemented as early as possible, beginning with the most critical links in the PCZ's.

5. The Panel wishes to point out that even when the spreading technology outlives its usefulness against the Soviet threat, it will still be viable in areas other than the PCZ's for a substantial period of time to provide privacy protection at low cost against less sophisticated intruders.

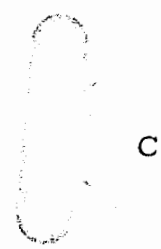
6. The Panel believes that the library of comsec technologies being developed by NSA will be applicable to protection of most domestic communication satellites. The Panel recommends that an appropriate mix of techniques be implemented on commercial satellite communications at the earliest possible date -- in parallel with protection of the terrestrial microwave network.

The Telecommunications Security Panel will be available to assist you and the transition group in any way we can with this important problem.

Sincerely,

Edward E. David Jr.

Edward David
Chairman, Special
NSC Panel on
Telecommunications Security



~~TOP SECRET~~ SENSITIVE 010046

Staff w/lay up done 010046

THE SECRETARY OF DEFENSE
WASHINGTON, D. C. 20301

(6491)

11 DEC 1976

MEMORANDUM FOR THE PRESIDENT

SUBJECT: NSA Report, 21 October 1976, An Assessment of Soviet Interception of Communications in the United States

I have reviewed the numerous actions under my purview concerning the problem of Soviet interception of communications in the United States. I believe we have charted the right course. The programs we are following and the technology we are applying should lead to satisfactory solutions to the problem; however, these solutions will take some time and entail substantial costs.

Pending the full implementation of these technological measures, I am not satisfied that we have sufficiently alerted all concerned to the seriousness of this problem, and to that end I am directing that programs to educate key Defense contractors on the Soviet threat to their communications be initiated.

I believe the overall matter is of sufficient importance to be discussed further at a meeting of the National Security Council at an early date.

Donald Rumsfeld

COPY 1 OF 6 COPIES.

~~TOP SECRET~~ SENSITIVE Sec Def Cont Nr. X-3478

D

ITEM WITHDRAWAL SHEET
WITHDRAWAL ID 01047

Collection/Series/Folder ID No.	:	004700174
Reason for Withdrawal	:	NS,National security restriction
Type of Material	:	MEM,Memo(s)
Creator's Name	:	Thomas Houser
Receiver's Name	:	Assistant for National Security Affairs
Description	:	re telecommunications security
Creation Date	:	12/09/1976
Volume (pages)	:	1
Date Withdrawn	:	05/25/1988

ITEM WITHDRAWAL SHEET
WITHDRAWAL ID 01048

Collection/Series/Folder ID No.	:	004700174
Reason for Withdrawal	:	NS,National security restriction
Type of Material	:	REP,Report(s)
Description	:	re telecommunications security
Creation Date	:	12/1976?
Volume (pages)	:	5
Date Withdrawn	:	05/25/1988

01049

~~TOP SECRET~~/XGDS

REPORT OF THE SPECIAL TASK GROUP ON TELECOMMUNICATION ORGANIZATION

December 1, 1976

~~TOP SECRET~~/XGDS-5(B)2
Classified by: Brent Scowcroft

BACKGROUND

NSDM 338 directed preparation of a plan describing actions necessary to achieve a wide degree of protection of private sector microwave communications, including needed policy and regulatory decisions as well as the detailed roles of industry and government in providing such protection. Implementation of these protective measures will be dependent on further Presidential review.

The Special Task Group on Telecommunications Organization, comprised of representatives of NSC, OMB, OTP, the Domestic Council, and the White House Counsel's Office, was formed to consider the need for and advisability of government organizational realignment should the President decide to implement such broad protection of private sector communications. The Task Group was asked to examine the possibility of realignment of existing organizations to provide focus to the overall telecommunications security program, as well as to consider the possibility of establishing a new government entity. The task group was asked to consider the following criteria in this evaluation:

1. Capability for analyzing and resolving technically and commercially complex telecommunications policy issues.
2. Capability for broad-based technical planning and program management.

Classified by: Brent Scowcroft

3. Recognized authority and ability to act in a government wide role.

4. Ability to budget and obligate sufficient funds.

5. Ability to attract competent personnel.

6. Access to intelligence and communications security community.

THE THREAT

The Soviets are using their Embassy and other diplomatic locations in Washington, New York, and San Francisco to conduct an extensive and growing microwave intercept program to listen in on the telephone conversations of government agencies, government defense contractors and U. S. businesses. The information collected by this intercept program is exploited by the Soviets to gain insight into critical U. S. Government decisions, new developments in military weapons, and proprietary and classified military technology, as well as to exploit the U. S. in trade and monetary transactions.

The Government has already taken actions to protect the more sensitive government and government defense contractor communications by moving them to less vulnerable cable circuits in the known threat areas. More extensive measures to protect all microwave circuits in the known threat areas are now being considered. Beyond this lies the larger problem of coping with other foreign and domestic threats to microwave and satellite communications nationwide. The solution to this problem is likely to be a gradual process involving a number of steps over time to provide increased protection.

THE GOVERNMENT ROLE

The Government role in this process is still being considered. Some Government involvement is clearly appropriate since the Government has a responsibility to improve security for its own communications and for the communications of its defense contractors. Further, the Government is the sole repository of the essential cryptographic technology and the Government must provide policy, standards, and regulations if the nation is to retain a truly integrated telephone system--that is, a system where any user can talk to any other user. Lastly, the Government should be in a position to select the proper balance between release of critical comsec technology to protect domestic telecommunications and control of comsec technology transfer to avoid foreign government interference with critical U. S. intelligence-gathering functions overseas. It is particularly important for the Government to create a favorable climate for public acceptance of communications security so that it is perceived as a means to increased privacy and not as a threat.

It would be possible to accomplish the needed security through a Federally-mandated program to protect the domestic telecommunications network. Such an approach may allow more rapid implementation of needed security measures but would require major Government intervention into the operations of the telecommunications industry, as well as requiring the Government to make politically sensitive choices of which elements of the private sector would be protected and which would not.

An alternative approach would be to emphasize a program of privately managed and financed secure communications services offered competively by the commercial communications carriers with the costs to be borne by the users. The Government role would be oriented towards establishing policy, standards, and regulations; making basic cryptographic technology available to stimulate its application in the commercial sector; establishing policy for controlling diffusion of this technology; using approved commercially provided secure communications for government agencies and sensitive government contractors (thereby providing necessary improvements in government communications security as well as creating a market demand for commercially provided secure communications services); and conducting an educational campaign to make the private sector aware of the nature and scope of the threat as well as the availability of government approved secure communications services.

These options are currently under study by OTP in response to NSDM 338. Presidential review and decision is expected before an approach is selected.

Whichever approach is selected, there will be cost and competitive impact on the commercial telecommunications carriers. The allocation of cost of protection between government and private sector, as well as among carriers, raises a number of issues which are not yet fully resolved. The unprecedented nature of protecting microwave transmissions along with

the uncertainties inherent in research and development efforts do not provide historical cost figures upon which to base cost estimates with a high degree of confidence.

The program will also impact on national policies favoring competition in private line common carrier services. The other common carriers competing with AT&T may be disadvantaged if they are required to fund this program because: (1) the long-haul transmission facilities of the other common carriers are overwhelmingly microwave, requiring protection; (2) such common carriers compete directly with AT&T for all of their business and may be unable to recover all of their costs from increases in revenue; and (3) several of the smaller common carriers are already suffering cash flow and capital problems.

A systematic solution to these problems must, by its nature, involve numerous government agency and private sector interests. There is currently no single organizational or administrative structure within the government capable of addressing this problem.

THE PLAYERS

The telecommunications security problem cuts across conventional organizational boundaries between economic and national security matters and between domestic and foreign affairs. The interests of many organizations are directly affected by the threat and the choice of responses.

NSA, the intelligence community, and the Department of Justice have all been directly involved in assessing the threat. NSA and other Defense Department elements (DTACCS, DCA, NSC) have been responsible for developing and implementing the protective technologies. NSA is the sole repository of cryptographic and communications security know-how. The Office of Telecommunications Policy has interests in the policy, legal, common carrier, and legislative areas, and the Department of State has interests in foreign policy issues. As measures are implemented to protect telecommunications on a broader scale, this list of organizations will expand to include the FCC, the Department of Commerce, the commercial communications carriers (including AT&T, the independent telephone companies, Western Union, and the domestic satellite carriers) and the entire body of communications users desiring security, including most government agencies as well as many elements of the private sector. Also, when the question of the appropriate role of Government in securing U. S. telecommunications is made public, Congress will become very much involved in determining our response.

To date the government responses to the telecommunications security problem have been focused and guided by the NSC, with the assistance of a special ad hoc advisory panel comprised of representatives of NSA, other DOD elements (DTACCS and DCA) and OTP, as well as several non-government technical consultants. A more permanent mechanism is needed whereby the

longer-term solutions can be implemented in an orderly and timely fashion. This organization will have to respond to the needs of the national security community, other government interests, and the interests of the private sector--both as users and suppliers of secure communications.

A MANAGEMENT CONCEPT

The fundamental management issue is how the Government should be organized to adequately cope with the complex issues involved as well as to effectively make use of the total resources of the Government and private sector in counteracting attempts at domestic communications interception.

The functions to be performed by the Government will depend on the government role but would likely include resolution of policy issues, setting standards, establishing programmatic and budgetary priorities, developing basic technology, controlling diffusion of communications security technology and/or equipment, and providing an overall focus for system planning and design.

While there are a large number of government organizations with interests in the communications security area, none of these organizations are currently equipped to deal with implementation of communications security measures on a widespread basis. Certain organizations must have a strong continuing role irrespective of the nature of the program. For example, the National Security Agency is responsible on a government-wide basis for the development and manufacture of cryptologic devices, and is an

essential contributor to the strong technology base which is critical to the success of the program. However, the political sensitivity of many of the issues, involving questions of individual privacy and new economic burdens on consumers, may make it inadvisable to assign sole responsibility to an agency so closely connected with the military and intelligence community.

A central focus organization is needed for policy formulation and coordination, and to oversee and bring together the resources of government and industry toward a long-term communications protection program. Such an organization would take a leadership role and coordinate the efforts of other government departments and agencies and the civilian sector. It would conduct overall planning for protection of the national telecommunications system, keep the National Security Council apprised of progress, and would have the Executive Agent function for telecommunications protection with responsibility to assure that telecommunications policy and regulatory actions are consistent with the program concepts. It would assess the status of technological developments, ensure that budgetary and funding channels are defined, establish liaison and communications channels with government agencies and with appropriate congressional committees, as well as maintaining continuous and open dialogue with non-government and private sector organizations associated with and participating in this program. The concept of an Executive Agent would be a viable method of mobilizing

the total resources necessary to support such a national program. It allows for participation of both the involved government agencies and elements of the civil sector. The relationship of the Executive Agent to the other major players is shown in Figure 1. The primary players are in the inner ring, and the secondary players are in the outer ring.

ORGANIZATIONAL ALTERNATIVES

The authority, visibility, and location of the Executive Agent will have a significant impact on its ability to deal effectively with the wide range of government, civil, and industry participants. The location of this organizational focus will also affect the public acceptance of such a program. The government must explain the need for improved communications security in a way which promotes public understanding that the technical solutions are in the public interest and are not perceived as threat to individual privacy. This implies Presidential involvement in the issue.

There are six organizational alternatives for fulfilling the role of the central focus. They are:

~~CONFIDENTIAL~~

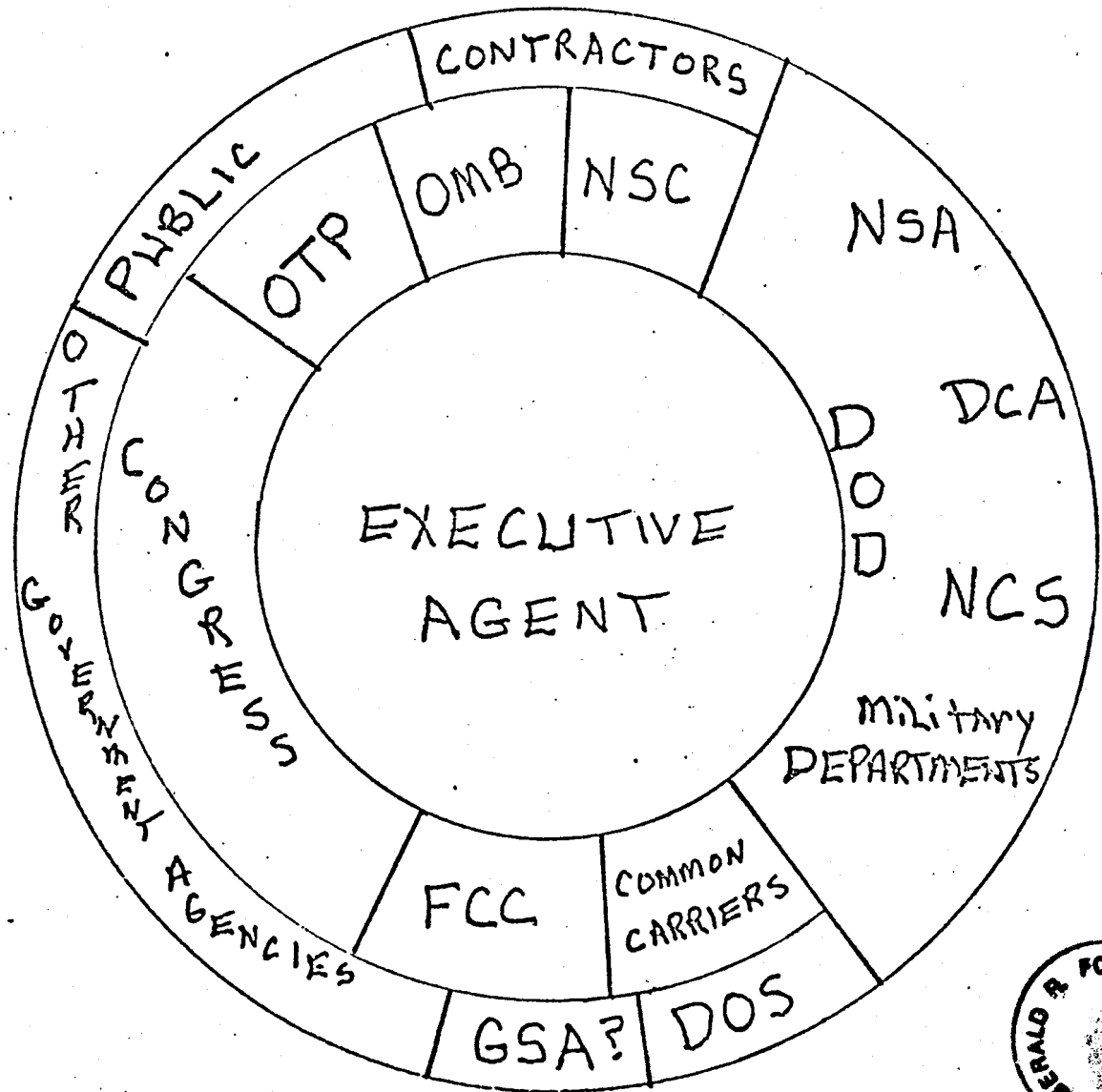


Figure 1

Executive Agent Relationships

~~CONFIDENTIAL~~

1. A specially designated cabinet committee reporting to the President, supported by a private sector advisory board.

Such a cabinet committee, chaired by a department head, possibly by the Secretary of Defense, would be supported by a small permanent staff (10-15 members) for policy planning, legal and economic studies, system planning, and coordination of government wide actions. Major program elements would be budgeted and implemented within existing departmental or agency organizations. A private sector advisory board of industry and public members could represent the interests of the telecommunications carriers, the telecommunications users, and the public at large.

Pros:

-- Would provide high-level consensus on policy questions and would have good access to the President.

-- Would command resources of agencies represented.

-- Would give high-level focus, while insulating the President from direct management of the program.

-- Has good access to the intelligence and communications security community.

-- Could reduce implications of military/intelligence involvement if chaired by some one other than the Secretary of Defense.

-- Advisory Board of industry and public members would help place the program in proper perspective with the private sector and public at large.

-- Has good access to competent personnel for initial staffing.

Cons:

-- The interest of cabinet members might wane under the press of urgent departmental responsibilities.

-- No mechanism would exist to reconcile differences without direct appeal to the President.

-- Personnel changes could cause discontinuity.

2. A joint government committee located in the Office of the Vice President supported by a private sector advisory board

Such an interdepartmental committee, chaired by the Vice President, would be supported by a small permanent staff (10 to 15 members) located in the office of the Vice President for policy planning, legal and economic studies, system planning, and coordination of government wide actions. Major program elements would be budgeted and implemented within existing departmental or agency organizations. A private sector advisory board of industry and public members could represent the interests of the telecommunications carriers, the telecommunications users, and the public at large.

Pros:

-- More likely to retain high-level interest over the long term.

-- Authority of Vice President would provide increased stature and priority for application of agency resources.

-- Would give high level focus on policy questions, while insulating President from direct management of the program.

-- Would reduce implications of military/intelligence involvement.

-- Advisory Board of industry and public members could help place the program in proper perspective with the private sector and public at large.

Cons:

-- A competent policy and technical planning staff would have to be established.

3. Continuation of National Security Council oversight of the program.

This approach would continue the existing oversight mechanism, using a very small staff within the NSC (1 to 2 members) to formulate policy and coordinate actions of other government agencies. Major studies and program implementation would have to be accomplished by resources of existing government organizations.

Pros:

-- Recognized authority with existent policy coordination capabilities.

-- Good access to the President.

-- Good access to intelligence and communications security community.

Cons:

-- Not a desirable location for day-to-day operating responsibilities

-- No depth in telecommunications matters.

-- Constraints on staff size would severely limit technical and policy planning capability.

-- Draws attention to "national security" implications of the program, which may be undesirable.

4. Designation of a single cabinet office to implement the program

In this option a single cabinet office, most likely DOD, would be responsible for all aspects of the program, including policy planning, legal and economic studies, budgeting, technical developments and implementation. Existing comsec technical and policy functions would be consolidated under a senior individual within DOD.

Pros:

-- Unity of command and resources within one department.

-- Existent technical capability.

-- Direct budgeting authority.

-- Good access to intelligence and communications security community.

Cons:

-- Policy decisions could be biased by narrow mission responsibilities of the department.

-- Interest and priority might wane under press of other departmental responsibilities.

-- Public perception of the program might be colored by the direct connection to military/intelligence organization.

-- Only recourse to resolve disputes between agencies would be direct appeal to the President.

5. Formation of a new organization in the Executive Branch reporting to the President.

Formation of a new organization in the Executive Branch would consolidate all the policy, regulatory, and technical functions related to private sector communications security, including existing comsec organizations, in one location. The staff for such an organization would be somewhat larger because of the need to provide administrative supporting functions.

Pros:

-- Location, staff skills and inter-agency relationships can be optimized for this problem.

-- New agency would be insulated from other priorities which can divert attention from new mission.

-- Minimized "image" problem associated with military/intelligence organizations.

-- Area budgeting authority.

Cons:

-- Time-consuming and difficult to establish; legislation likely to be required.

-- Furthers proliferation of small, special purpose government organizations.

-- Ability to maintain cooperation of major agencies may wane, particularly if access to the President is not available either directly or through a major presidential staff officer.

-- Access to intelligence community would have to be established.

-- Likely to create overlaps with responsibilities of existing organizations.

6. Designation of an existing office in the Executive Branch reporting to the President

All policy and regulatory functions related to communications security could be consolidated in an existing organization in the Executive Branch such as OTP. Major technical elements of the program would be implemented through existing DOD agencies. A staff of 10-15 would be required to support this function.

Pros:

-- Start-up time would be minimal because of existing working relationship with other government agencies and communication channels with industry and public interest groups.

-- Existent policy planning capability.

Cons:

-- OTP and other existing agencies like the Office of the Science Adviser have no capability or experience in program implementation.

-- Pressure to restrain the size of Executive Branch offices may lead to assignment of the minimum set of responsibilities and minimal personnel, weakening the central focus.

-- Likely to create additional overlaps with responsibilities of existing organizations.

-- Ability to maintain cooperation and resources of major agencies may wane, particularly if access to the President is not available either directly or through a major presidential staff officer.

TASK FORCE OBSERVATIONS

The Special Task Group believes it would be inappropriate to recommend any of the organizational alternatives discussed previously to a new Administration. We have developed, however, several observations and suggested criteria which we believe should be considered in selecting a central focus organization, if it is to successfully carry out its task of implementing a nationwide communications security system. These observations are as follows:

-- If the extent of the government role in implementing the communications security program is limited and emphasis is placed on privately managed and financed measures, then one of the first three options would be more appropriate for the central focus of the government organization, and major changes in the responsibility of other government agencies would not be necessary. If, on the other hand, a more aggressive government role is selected, then one of the last three options would be more appropriate and it would be necessary to consolidate and restructure existing agencies to a greater degree.

-- A voluntary cooperative partnership between the Federal Government and the common carrier industries would be preferable to a potentially contentious Federally mandated program.

-- The national communications security program should be implemented so that it permits maximum competition between industries in accordance with our private enterprise system. It should avoid according unfair advantage to one carrier over another.

-- The organizational focus should include a consultative mechanism at a sufficiently high level to expeditiously resolve policy disputes between Federal agencies and to provide necessary authority to carry out policy decisions.

-- The organizational focus must have sufficient staff resources with highly specialized skills in the key policy and technical areas to carry out its functions.

-- The program will receive greater public acceptance if the organizational focus is not perceived as an extension of the military/intelligence organizations of the Federal Government.

-- The organizational structure must, however, allow for the full participation and cooperation of the National Security Agency.

-- The organizational structure should also provide a mechanism to represent the interests of the private sector, possibly through an advisory board of industry and public members selected from the telecommunications carriers, the telecommunications users, and the public at large.

These observations lead the Task Group to favor either a Cabinet Committee (Option 1) or a government committee in the Office of the Vice President (Option 2). It is the opinion of the task group that continuation of NSC oversight (Option 3) would be ineffective because of staff size limitations. Designation of DOD (Option 4) or a new Executive Branch organization (Option 5) for program management should only be considered if a large-scale Federally mandated program were selected. Designation of OTP or similar existing Executive Branch agency (Option 6) would not be effective because the interest and cooperation of other government agencies would be likely to wane if OTP does not have ready access to the President.