NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

~~TOP SECRET/SENSITIVE~~

August 15, 1974

National Security Decision Memorandum 266

TO: The Secretary of Defense

SUBJECT: Improved Security of Telecommunications

The President has been informed of the opportunities for Soviet interception of critical unencrypted Government telephone conversations which may be carried on Washington area microwave links. He has directed that immediate defensive steps be taken to counter this situation.

In that connection, he has directed that you develop, in coordination with the Assistant to the President for National Security Affairs and the Director of the Office of Telecommunications Policy, a specific program designed to reduce significantly the opportunities for such interception.

The program should include near term interim measures including steps to route critical Government communications on cables or wire lines until well out of the Washington area. It also should propose more comprehensive long term measures including but not limited to expansion of the availability of secure telephones useable over standard telephone lines, and alternative programs for securing the microwave links in the Washington area. Program definition for both near term and longer term proposals should include technical descriptions, costs, and scheduling information assuring highest priorities.

Details as to specific near term interim measures which can be or are being instituted and the specific dates on which they will become effective should be submitted to the President for his consideration not later than October 1, 1974. Details of longer term measures for this program should be submitted for the President's consideration not later than January 1, 1975.

Henry A. Kissinger

cc: The Deputy Secretary of State
The Director, Office of Management and Budget
The Director of Central Intelligence
The Director, Office of Telecommunication Policy

DECLASSIFIED

~~TOP SECRET/SENSITIVE~~ /XGDS

Authority NSC letter, 4/16/96
By LL NLF Date 4/7/97

DECLASSIFIED
E.O. 13526 (as amended) SEC 3.3
MR # 07-111; #4
NSC letter 7/15/11
By dal NARA, Date 9/13/11

6082X

THE WHITE HOUSE

WASHINGTON

INFORMATION

~~TOP SECRET~~/SENSITIVE

December 17, 1974

MEMORANDUM FOR: THE PRESIDENT

FROM: HENRY A. KISSINGER

SUBJECT: NSDM 266

You may recall that shortly after you took office this fall, I advised you that the Soviet Union was actively intercepting US government telephone conversations carried by microwave in the Washington area, principally from the Soviet Embassy, but probably from other sites as well. The volume of intercept was quite large, and since sensitive information from key government agencies could be readily derived from aggregation and analysis of these conversations, I recommended that you approve a NSDM directing corrective action. NSDM 266 directed the Secretary of Defense to take immediate steps to reduce opportunities for Soviet intercept of government telephone communications via microwave in the Washington area. Near term actions were to be identified by October 1, and longer term measures by January 1.

The October response identified 10,000 leased government circuits terminating in the Washington area for which protection seemed prudent. About 4,000 of these circuits are now on microwave and exploitable, and the remaining 6,000 are already on cable but must be tagged to see that they remain there.

We have already initiated action to move the radio circuits to cable beginning in December. Initial estimates are that the entire moving/tagging process will be complete by next August, but we are working closely with AT&T management to accelerate this schedule. A much earlier completion date should be possible. Work on longer term measures to more thoroughly eliminate significant Soviet intercept opportunities is continuing and seems to be on schedule for a January 1 submission.

~~TOP SECRET~~/SENSITIVE XGDS 3

GERALD R. FORD LIBRARY

THE WHITE HOUSE

WASHINGTON

December 17, 1974

Dear Bill:

I have recently been apprised of near term actions taken in response to NSDM 266, and of your personal efforts in support of this action. I wanted to let you know that I am extremely pleased with the rapid progress that has been achieved, and to express my sincere appreciation for your major contribution to this progress.

Best regards,

Henry A. Kissinger

Dr. William O. Baker
Vice President for Research
Bell Telephone Laboratories
Murray Hill, New Jersey 07971

dispatched for WB 12-17-74

MEMORANDUM

NATIONAL SECURITY COUNCIL

~~TOP SECRET~~/SENSITIVE

ACTION
6082X

December 12, 1974

MEMORANDUM FOR: SECRETARY KISSINGER

FROM: GORDON O. MOE

THROUGH: RICHARD KENNEDY

SUBJECT: Presidential Summary of NSDM 266 Status

Ref: Action 5860X

Attached per your request are:

- A revised memorandum to the President summarizing status of NSDM 266 actions (Tab A).
- A letter thanking Dr. Baker for his assistance on this matter (Tab B).

DECLASSIFIED
E.O. 13526 (as amended) SEC 3.3
MR # 07-111; #6
NSC ltr 7/15/11
By dal NARA, Date 9/13/11

GERALD R. FORD LIBRARY

~~TOP SECRET~~/SENSITIVE XGDS 3 Classified by: Gordon Moe

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

DECLASSIFIED
E.O. 13526 (as amended) SEC 3.3
NSC Memo, 3/5/2013, State Dept. Guidelines
By NLO, NARA, Date 1/6/2012
and FRUS Vol. E-3, Documents on Global Issues, Doc. 109

~~TOP SECRET~~/SENSITIVE/XGDS-3 May 23, 1975

National Security Decision Memorandum 296

TO: The Secretary of Defense
The Deputy Secretary of State
The Director, Office of Telecommunications Policy
The Administrator, General Services Administration

SUBJECT: Improved Communications Security

The President has reviewed the status of near term actions DOD has taken in response to NSDM 266 and the alternative longer term solutions proposed. The President concurs in the near term actions already underway to move critical Washington area government circuits to cable and encourages continued efforts to accelerate these steps to completion.

It is recognized that an award may have to be made in GSA's on-going competitive procurement of 166 microwave circuits between New York and Washington. If the Administrator, GSA, concludes that an award should be made, the President desires that the risk of disclosure of the Soviet intercept problem be minimized. Therefore, NSA and OTP should develop criteria permitting maximum utilization of such circuits, while still protecting sensitive information, and GSA should be prepared to cover the cost of any unused circuits.

Prior to making decisions regarding implementation of long term measures, the President has requested additional studies and information. Specifically, a DOD plan for implementing the Washington Protected Communications Zone (PCZ) should be submitted by October 1, 1975. Since broad Soviet intercept of major private firm communications is also a matter of concern, the plan should include costs and schedules of alternatives for securing (a) all commercial links in the PCZ, as well as (b) only the portion of commercial links likely to be leased by the government. A preliminary analysis of the boundaries, structure, and priority of PCZs in other major cities of potential concern should also be completed by this date. DOD should also submit a detailed implementation plan for an Executive Secure Voice Network by September 1, 1975. The plan should include a costs schedule for accelerated introduction of this service, and should propose alternatives for expanding

the service both in and beyond the Washington area and for achieving interoperability with other secure voice systems. Pending completion of these studies and plans, and the issuance of further guidance, the President directs that there be no increase in the level of exposure of sensitive traffic to microwave interception in those cities which are candidates for future designation as PCZs.

The DOD should immediately undertake development of Protected Radio Modulation technology to support the PCZ concept, and should accelerate development of narrow band secure voice terminals and compatible key distribution technology to facilitate implementation of an interim operational ESVN capability as early as mid-1977.

Single channel radio circuits in the Washington PCZ should be secured at the earliest possible time, and DOD should submit an implementation plan for securing single channel satellite links terminating in the Washington PCZ by October 1, 1975.

If it is decided to implement the Washington Microwave Interconnect, the system should be designed to be fully secured at the outset, whether it is government owned or leased.

Approval is deferred on proposed long term measures and developments not addressed in this decision memorandum pending completion of the PCZ and Executive Secure Voice Network implementation plans. However, FY 1976/1977 DOD budget allocation/planning should reflect the possible need for support of concept implementation and additional supporting R&D.

The State Department is requested to review potential political implications of implementing the PCZ concept, and OTP is requested to develop proposals to permit expanded implementation of the PCZ concept with minimal risk of public disclosure of the Soviet intercept problem.

Brent Scowcroft
Henry A. Kissinger /cz

cc: Director, Office of Management and Budget
The Director of Central Intelligence
The Director, National Security Agency

Gen. Scowcroft

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

~~TOP SECRET~~/XGDS

July 7, 1976

National Security Decision Memorandum 333

TO: The Secretary of Defense
The Director of Central Intelligence

SUBJECT: Enhanced Survivability of Critical U.S. Military and Intelligence Space Systems

The President has expressed concern regarding the emerging Soviet anti-satellite capability and the possible threat to critical U.S. space missions this implies. He considers preserving the right to free use of space to be a matter of high national priority. The U.S. trend toward increasing exploitation of space for national security purposes such as strategic and tactical reconnaissance, warning, communications, and navigation -- combined with the simultaneous trend toward a smaller number of larger, more sophisticated satellites -- emphasizes the need for a reassessment of U.S. policy regarding survivability of critical military and intelligence space assets.

Policy for Survivability of Space Assets

The President has determined that the United States will continue to make use of international treaty obligations and political measures to foster free use of space for U.S. satellite assets both during peacetime and in times of crisis. However, to further reduce potential degradation of critical space capabilities resulting from possible interference with U.S. military and intelligence space assets, the President also considers it necessary to implement improvements to their inherent technical survivability. Such survivability improvements should supplement and reinforce the political measures, as well as extend the survivability of critical space assets into higher level conflict scenarios.

The survivability improvements in critical military and intelligence space assets should be predicated on the following U.S. objectives:

(1) Provide unambiguous, high confidence, timely warning of any attack directed at U.S. satellites;

~~TOP SECRET~~/XGDS

DECLASSIFIED • E.O. 12958 SEC. 3.6
WITH PORTIONS EXEMPTED
E.O. 12958 SEC. 1.5

MR 04-63, #2; NSC ltr 6/27/06

BY dal NARA DATE 2/6/09

(2) Provide positive verification of any actual interference with critical U.S. military and intelligence satellite capabilities;

(3) Provide sufficient decision time for judicious evaluation and selection of other political or military responses after the initiation of an attempt to interfere and before the loss of a critical military or intelligence space capability;

(4) Provide a balanced level of survivability commensurate with mission needs against a range of possible threats, including non-nuclear co-orbital interceptor attacks, possible electronic interference, and possible laser attacks;

(5) Substantially increase the level of resources needed by an aggressor to successfully interfere with critical U.S. military and intelligence space capabilities;

(6) Deny the opportunity to electronically exploit the command system or data links of critical U.S. military and intelligence space systems.

Planning for Improved Survivability

The President directs that efforts be initiated jointly by the Secretary of Defense and the Director of Central Intelligence to prepare an aggressive time-phased, prioritized action plan which will further develop and implement this policy framework. This plan should (1) place emphasis on short-term and intermediate-term measures to enhance the survivability of critical military and intelligence space capabilities against Soviet non-nuclear and laser threats at low altitudes and Soviet electronic threats at all altitudes, and (2) consider long-term measures which will provide all critical military and intelligence space systems with a balanced level of survivability commensurate with mission needs against all expected threats, including threats at higher altitudes.

Short/intermediate term measures for consideration in the plan should include, but not be limited to, the following capabilities:

(1) .....
.....
.....
.....
.....
.....
.....

(2) .....

(3) .....

(4) .....

Longer-term measures should provide balanced survivability for critical space capabilities against the full range of credible threats. The plan should detail the military and intelligence utilization of specific systems at various levels of potential conflict and should select survivability measures and implementation schedules for each critical military or intelligence satellite in accord with their scenario-related mission needs. The threats to be considered include threats of physical attack against satellites, either by non-nuclear or laser techniques; electronic and exploitation threats against command links, data links, and communications links; and threats of electronic or small-scale physical attack against ground stations. Continued consideration should be given to protection against nuclear effects from events other than direct attack, for those space assets which support nuclear scenarios. This portion of the plan should consider measures necessary to enhance the survivability of both ground and spaceborne elements and should consider proliferation or back-up alternatives where appropriate, as well as active and passive measures.

The plan should develop a range of implementation schedule/funding profiles for Presidential consideration. An initial version of this plan should be submitted to the President no later than November 30, 1976.

Brent Scowcroft

cc: The Secretary of State
The Chairman, Joint Chiefs of Staff
The Director, Office of Management and Budget

GERALD R. FORD

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

~~TOP SECRET~~/XGDS

September 1, 1976

DECLASSIFIED
E.O. 13526 (as amended) SEC 3.3
MR # 07-111; #7
NSC letter 7/15/11
By dal NARA, Date 9/13/11

National Security Decision Memorandum 338

TO: The Secretary of Defense
The Director, Office of Telecommunications Policy

SUBJECT: Further Improvements in Telecommunications Security (TS)

The President has reviewed the status of measures to protect government telephone communications in the Washington, D.C., New York City, and San Francisco areas taken in response to NSDM 266, NSDM 296, and other directives. He directs that actions now underway to move critical circuits from microwave to cable in the New York City and San Francisco locations be given high priority and that development of Protected Radio Modulation (PRM) techniques for earliest possible application in known threat areas be expedited.

The President is concerned about possible damage to the national security and the economy from continuing Soviet intercept of critical non-government communications, including government defense contractors and certain other key institutions in the private sector. The President further recognizes that U.S. citizens and institutions should have a reasonable expectation of privacy from foreign or domestic intercept when using the public telephone system. The President has therefore decided that communication security should be extended to government defense contractors dealing in classified or sensitive information at the earliest possible time. He has also directed that planning be undertaken to meet the longer-term need to protect other key institutions in the private sector, and, ultimately, to provide a reasonable expectation of privacy for all users of public telecommunications. Implementation of these longer-term plans will be dependent upon further Presidential review.

Toward these objectives, the President desires that action be taken by the Secretary of Defense to accomplish the following:

1. Immediate steps should be taken to reduce vulnerability to Soviet intercept of private line communications of government contractors dealing in classified or sensitive information. Action should be

taken as soon as possible to move circuits of critical government defense contractors from microwave to cable in confirmed threat areas. This action should be accomplished without further disclosure of Soviet intercept operations. Procedures for moving circuits should be modeled after procedures used to implement NSDM 266. The Department of Defense shall cover the cost of moving and securing these circuits. Only those circuits on carriers offering alternate cable routing shall be moved. Selection and priority of circuits to be moved shall be established by DOD based on sensitivity of classified contracts and intelligence information on Soviet intercept operations.

2. In order to preserve an option to initiate jamming quickly, action should be taken to develop contingency plans, procure necessary equipment and acquire necessary real estate locations to allow jamming on short notice of Soviet intercept operations at the Soviet Embassy in Washington, D. C., the Soviet Mission to the United Nations in New York City, the Soviet Consulate in San Francisco, and the Soviet residential complex in Riverdale, New York.

The President further directs the Director of the Office of Telecommunications Policy, with the participation and assistance of DOD and NSA, to prepare a detailed Action Plan setting forth the actions and schedule milestones necessary to achieve a wide degree of protection for private sector microwave communications. The Plan should identify needed policy and regulatory decisions, describe in detail the roles of industry and government, including management and funding considerations, and integrate the schedule for these actions with the technical development milestones.

This Plan should be divided into two distinct phases. Phase I shall at the earliest possible date provide for protection of those microwave radio links in Washington, D. C., New York City, and San Francisco which are most vulnerable to exploitation by the Soviet Union, with extension to the complete Washington, New York, and San Francisco Protected Communications Zones (PCZs) as soon thereafter as feasible. Phase II shall provide for longer-term protection of domestic microwave communications on a nationwide basis. Protection shall be accomplished without excessive government intrusion into the private sector. The approach to securing microwave communications against interception in Phase II should be to encourage the commercial telecommunications carriers to provide protected service offerings with the costs of protection borne by the users. The government role should be oriented towards establishing policy, regulations, and standards, as well as developing basic

technology as a stimulant to the commercial sector. The approach to securing the PCZ microwave links in Phase I shall be consistent with a smooth transition to broader application in Phase II. The Plan should consider all of the technical solutions for reducing foreign or domestic microwave intercept defined by the Washington, D. C., PCZ Implementation Plan being prepared by the Department of Defense.

The Action Plan should be based on the fundamental objective of protecting the privacy of all users of public telecommunications, as well as satisfying specific needs of the government. It should include a full statement of the legal, political, economic and social basis for this objective and should present in detail the related policy, regulatory and legislative actions which must be taken by various government agencies to achieve the desired protection. The Action Plan should also provide a strategy and detailed plan for public explanation of government actions for both Phases I and II. The Action Plan should be submitted for consideration by the President no later than 30 November 1976.

Brent Scowcroft

cc: Secretary of State
Director of Central Intelligence
Director, National Security Agency

770 6776-X

NSDM 346

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

~~TOP SECRET~~/XGDS

January 18, 1977

PHOTOCOPY FROM GERALD FORD LIBRARY

National Security Decision Memorandum 346

TO: The Vice President of the United States
The Secretary of State
The Secretary of Defense
The Attorney General
The Secretary of Commerce
The Director, Office of Management and Budget
Counsel to the President
Assistant to the President for National Security Affairs
Assistant to the President for Domestic Affairs
The Director of Central Intelligence
The Chairman, Federal Communications Commission
The Director, Office of Telecommunications Policy

SUBJECT: Security of U. S. Telecommunications

The rapid growth in the use of microwave radio in our long distance telephone system has greatly increased the vulnerability of our telephone communications to foreign or domestic intercept. These microwave links are open and can be intercepted and recorded with relative ease using comparatively inexpensive, small, and unobtrusive equipment. It is possible, therefore, that intercept operations in the US could be conducted either by foreign countries or criminal elements. The President is concerned about this threat and has directed the following actions to deal with it.

-- Government communications in the Washington area have been rerouted from microwave to cable, and government communications in New York and San Francisco are in the process of being moved to cable.

-- The lines of sensitive government contractors are similarly being shifted to cable.

-- The Department of Defense has developed electronic bulk scrambling techniques that can protect microwave links on a comprehensive basis at relatively low cost. A system will be installed and tested on a major link in Washington during the course of this year.

GERALD R. FORD LIBRARY

DECLASSIFIED
AUTHORITY NSC Memo 4/20/05
BY ldr NLF, DATE 7/5/05

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

PHOTOCOPY FROM GERALD FORD LIBRARY

-- The Office of Telecommunications Policy (OTP) has prepared an implementation plan for use of these electronic scrambling techniques on all microwave links in the three areas of Soviet interception activity, and a second phase to introduce this protection nationwide.

After reviewing the status of these actions and the recent recommendations of the National Security Council (NSC), the Domestic Council, and the White House Counsel, the President has decided that the program to protect US telecommunications should proceed as an urgent matter.

New Oversight Committee

To assure continued priority attention to this important matter throughout the executive branch, the President has directed the establishment of a joint NSC/Domestic Council Committee on the Security of US Telecommunications, to be chaired by the Vice President. The membership will include the addressees and such additional members as the Vice President may consider appropriate. The Committee, inter alia, will:

-- Provide oversight and coordination of measures in implementation of this policy.

-- Report periodically to the President on the implementation of the protection program.

-- Serve as the point of contact for interchanges with the Congress, the Federal Communications Commission, the common carriers and communication industry, and others as appropriate.

Next Steps

The OTP implementation plan for wide scale application of communication protection is predicated on the selection of one of two major alternatives for the government/industry role.

-- The first alternative would minimize the government role through a cooperative government/industry effort. The government would require government agencies and sensitive government contractors to use approved commercially provided secure communication services. This would create a substantial market demand for secure communications as well as provide needed improvement

GERALD R. FORD LIBRARY

PHOTOCOPY FROM GERALD FORD LIBRARY

in security of government communications. It would be anticipated that, once established, market forces combined with greater public awareness would work to assure broad application of telephone security. The advantage of this alternative is the minimal governmental role, but a significant drawback is the lack of certainty that such broad protection would in fact materialize.

-- The second alternative provides for government action through a Federally-mandated program directing implementation of approved protection techniques throughout the national microwave network. This approach would require implementing legislation and could require the government to make choices as to which sectors of the private sector would be protected.

In both these alternatives, the government would establish policy, standards and regulations, would assist the private sector by making government-developed cryptographic 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 as well as the commercial availability of government-approved secure communications. Industry would apply bulk protection techniques to the communications networks and would pass the added costs on to the users.

As a first order of business, the Committee is requested to evaluate these options and to make recommendations to the President by March 1, 1977. This report should include drafts of any proposed legislation and a plan for public disclosure and the elicitation of public support.

Brent Scowcroft

cc: Director, National Security Agency

GERALD R. FORD LIBRARY