

Declassified in Part - Sanitized Copy Approved for Release 2012/04/13 : CIA-RDP87B00342R000100070003-7

DDCI

SIG(I) Meeting re Counterintelligence

Tuesday, 17 December 1985, 1600 hours

Please return to ES

Declassified in Part - Sanitized Copy Approved for Release 2012/04/13 : CIA-RDP87B00342R000100070003-7

Central Intelligence Agency
Washington, D.C. 20505

Executive Secretariat

17 December 1985

NOTE FOR: DCI
DDCI

RE: SIG(I) on CI and Security Matters

Attached, at tabs, you will find:

- TAB A Revised agenda for today's meeting.
(Copies will be provided to attendees by IC Staff--due late hour, most likely when they arrive; however, calls have been made to those being called upon to alert them of changes.)
- TAB B List of those expected to attend.
- TAB C Copy of portion of Intelligence Authorization Act pertaining to "counterintelligence capabilities improvements report".
- TAB D Copies of exchange of correspondence between DCI and SecState re State lead in orchestrating overseas physical and technical security effort.



25X1
20A1

SECRET

TABLE OF CONTENTS

SIG-I MEETING, 17 DECEMBER 1985

- A. Agenda
- B. List of Speakers
- C. Talking Paper
- D. NSDD-196
- E. NSDD-145
- F. IG/CM Minutes
- G. IG/CI Minutes
- H. Task Force Minutes
- I. NTISSC Minutes

SECRET

A

CONFIDENTIAL

SIG(I) Meeting on Counterintelligence

Tuesday, 17 December 1985
Community Headquarters Building (Room 6W02)

REVIEW OF COMMUNITY COUNTERINTELLIGENCE AND SECURITY MATTERS

Agenda

- I. Introduction DCI (3 minutes)
- II. Summary of Recent Congressional Hearings on CI and Security DDCI (5 minutes)
- III. Presentation of Recent Activities/Future Plans of:
 - The IG/CI Judge Webster (5 minutes)
 - The IG/CM Craig Alderman (5 minutes)
 - The SECOM [Redacted] (5 minutes)
 - The NTISSC Don Latham (5 minutes)
 - The IHC [Redacted] (5 minutes)
- IV. Plans for Security of Overseas Facilities Robert Lamb (5 minutes)
- V. DoD Actions Flowing from Stilwell Commission Report General Stilwell (5 minutes)
- VI. COMSEC/^{COMPUSEC} Initiatives General Odom (5 minutes)
- VII. Administration Policy on Leaks Ken deGraffenreid (5 minutes)
- VIII. Status of Implementation of NSDD 196 (Task Force on Hostile Presence Options) David Major (5 minutes)
- IX. Discussion All (15 minutes)
- X. Summary DCI (2 minutes)

2:25X1

25X1
25X1

CONFIDENTIAL

SECRET

PROPOSED AGENDASIG-I MEETING, 17 DECEMBER 1985

The SIG-I will review key developments relating to:

- a. The recent Congressional hearings on counterintelligence and security, including a possible Counterintelligence Capabilities Improvement Report;
- b. The activities of various Intelligence Community components such as the SIG-I/IG system, pertinent DCI committees, and the National Telecommunications and Information Systems Security Committee, with particular reference to the status of critical CI and security issues such as the technical surveillance countermeasure upgrade program and US Embassy security; and
- c. The status of the NSC Implementation Task Force.

Representatives of pertinent Intelligence Community components will assist the SIG-I review by briefing appropriately on key developments.


The objective is to assist the SIG-I, which is at the top of the national CI/CM policymaking pyramid, in its ongoing integration and policy formulation across the entire counterintelligence and countermeasure spectrum.

SECRET

B

SECRET

SPEAKERS FOR SIG-I MEETING, 17 DECEMBER 1985

Judge Webster	IG/CI
Mr. Latham	NTISSC
General Stilwell	Defense Security
General Odom	NSA
Mr. Alderman	IG/CM
Mr. Lamb	State Security
Mr. deGraffenreid	Options/Leaks
	SECOM
	Information Handling Committee

25X1
20A1

SECRET

SECRET

TABLE OF CONTENTS

SIG-I MEETING, 17 DECEMBER 1985

- A. Agenda
- B. List of Speakers
- C. Talking Paper
- D. NSDD-196
- E. NSDD-145
- F. IG/CM Minutes
- G. IG/CI Minutes
- H. Task Force Minutes
- I. NTISSC Minutes

SECRET

A

PROPOSED AGENDA

SIG-I MEETING, 17 DECEMBER 1985

The SIG-I will review key developments relating to:

a. The recent Congressional hearings on counterintelligence and security, including a possible Counterintelligence Capabilities Improvement Report;

b. The activities of various Intelligence Community components such as the SIG-I/IG system, pertinent DCI committees, and the National Telecommunications and Information Systems Security Committee, with particular reference to the status of critical CI and security issues such as the technical surveillance countermeasure upgrade program and US Embassy security; and

c. The status of the NSC Implementation Task Force.


Representatives of pertinent Intelligence Community components will assist the SIG-I review by briefing appropriately on key developments.

The objective is to assist the SIG-I, which is at the top of the national CI/CM policymaking pyramid, in its ongoing integration and policy formulation across the entire counterintelligence and countermeasure spectrum.

SECRET

B

SPEAKERS FOR SIG-I MEETING, 17 DECEMBER 1985

Judge Webster	IG/CI
Mr. Latham	NTISSC
General Stilwell -	Defense Security
General Odom	NSA
Mr. Alderman -	IG/CM
Mr. Lamb -	State Security
Mr. deGraffenreid	Options/Leaks
	SECOM
	Information Handling Committee

Dave Major

25X1

SECRET

c

Page Denied

Next 2 Page(s) In Document Denied

SECRET

courses of action or refers issues to the NSC for implementation decisions.

In my mind, there is no question that the SIG-I structure not only has the right but the duty to monitor, review, and provide integrating policy guidance across the entire counterintelligence and countermeasure spectrum. So much for the larger picture. What I propose to do now in furtherance of my objectives for this meeting is to touch briefly and summarily on some of the key counterintelligence and countermeasure/security developments which have occurred during the past year or so. Then I would like representatives of pertinent Intelligence Community committees to assist by further briefing us appropriately.

25X1

SECRET

Page Denied

Next 8 Page(s) In Document Denied

D

~~SECRET~~

THE WHITE HOUSE

WASHINGTON

November 1, 1985

Executive Registry
85- 4195

UNCLASSIFIED
SECRET ATTACHMENT

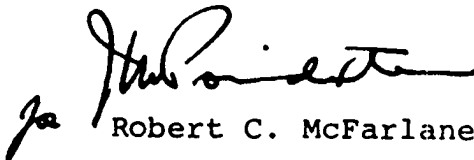
MEMORANDUM FOR THE VICE PRESIDENT
 THE SECRETARY OF STATE
 THE SECRETARY OF THE TREASURY
 THE SECRETARY OF DEFENSE
 THE ATTORNEY GENERAL
 THE SECRETARY OF COMMERCE
 THE DIRECTOR OF CENTRAL INTELLIGENCE
 CHAIRMAN, JOINT CHIEFS OF STAFF
 DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
 DIRECTOR, NATIONAL SECURITY AGENCY
 COMMISSIONER, IMMIGRATION AND NATURALIZATION
 DIRECTOR, US ARMY INTELLIGENCE AND SECURITY COMMAND
 COMMANDER, NAVAL INTELLIGENCE COMMAND
 COMMANDER, US AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS
 DEPUTY ASSISTANT SECRETARY OF STATE, DIPLOMATIC SECURITY SERVICE
 DIRECTOR, OFFICE OF FOREIGN MISSIONS

SUBJECT: NSDD on Counterintelligence/Countermeasures Implementation Task Force

The President has signed the attached National Security Decision Directive calling for the establishment of a task force to implement a number of policy decisions designed to limit the hostile intelligence presence in the US and place greater controls on movements. This task force will be chaired by David G. Major, Director of Intelligence and Counterintelligence Programs, National Security Council Staff.

Each recipient should designate a representative to participate on the task force and notify Mr. Major by November 8, 1985.

FOR THE PRESIDENT:


 Robert C. McFarlane

Attachment
NSDD -196

UNCLASSIFIED
SECRET ATTACHMENT

COPY 8 DE 17 COPIES
CIA

~~SECRET~~

SECRET

THE WHITE HOUSE

WASHINGTON

NATIONAL SECURITY DECISION
DIRECTIVE NUMBER 196

November 1, 1985

COUNTERINTELLIGENCE/COUNTERMEASURE IMPLEMENTATION
TASK FORCE (U)

Intelligence collection by foreign intelligence officers and agents operating in the United States presents the greatest counterintelligence (CI) threat confronting the United States. Under cover of diplomatic establishments, foreign-owned commercial entities and exchange student programs, the Soviet, Soviet Bloc, Peoples Republic of China and other criteria countries have emplaced large numbers of professional intelligence officers and other intelligence collectors (economic, scientific and technical, and military) in the United States. The numbers of foreign intelligence officers far surpass the counterintelligence assets the US Government has been able to deploy against them, and the number has been increasing over the years. This issue has been studied extensively by the Interagency Group on Counterintelligence (IG/CI) and a series of recommendations were forwarded to and endorsed by the Senior Interagency Group for Intelligence (SIG/I). These recommendations were reviewed and endorsed by the National Security Planning Group (NSPG) on August 7, 1985. I have decided it is in the national interest to implement each of these proposals. (U)

The NSPG also recommended that the US Government adopt, in principle, the use of aperiodic, non-life style, CI-type polygraph examinations for all individuals with access to US Government Sensitive Compartment Information (SCI), Communications Security Information (COMSEC) and other special access program classified information. I have decided this policy should be established. (U)

In order to facilitate the implementation of these decisions, I am directing the establishment of a task force to develop the time table, procedures and method to implement this Decision Directive. This implementation task force will be chaired by a representative of the Assistant to the President for National Security Affairs. The task force will be composed of a representative of each NSPG principal: Secretary of State, Secretary of Defense, Attorney General, Director of Central Intelligence, and Chairman, Joint Chiefs of Staff. In addition, the task force will include a representative of the Director of the Federal Bureau of Investigation and a representative from Department of State/Office of Foreign Missions (OFM). (U)

SECRET

Declassify: OADR

COPY 8 OF 17 COPIES
CIA**SECRET**

SECRET

2

The following agencies will provide an observer to this implementation task force since the timing and method of implementation may have an impact on one or more of them: Diplomatic Security Service (Department of State), Office of Foreign Missions (Department of State), Department of the Treasury, Department of Commerce, US Army Intelligence and Security Command, Naval Intelligence Command, US Air Force Office of Special Investigations, National Security Agency, and the Immigration and Naturalization Service. (U)

The Intelligence Community Staff Secretariat will provide necessary administrative support. (U)

The purpose of this task force will be to make recommendations on the method, timing and procedures to implement the SIG(I) options; establish implementation policy for the national polygraph program and implement other counterintelligence and countermeasures improvements which have appropriate national policy level implications. Final implementation decisions will be made by the President. (U)

The SIG(I) options to be implemented are:

Option #1: Equality in US and Soviet Bilateral Representation

Eliminate the disparity in US-USSR representation by July 1988. Accomplish this by undertaking a combination of initiatives to reduce the official Soviet presence in the US and increase the official US presence in the USSR. The Department of State will develop a plan to accomplish this objective. The NSC will review the schedule established to implement this plan and achieve equivalence. Advise the USSR that this is our policy and consider seeking agreement on the manner in which both aspects will be implemented. In the absence of agreement, implement the policy unilaterally to replace Soviet support personnel employed in the US establishments in the USSR and deny entry visas for replacement support personnel employed in Soviet establishments in the US until a balance is achieved between the number of US and Soviet personnel with diplomatic immunity.

(S)

(b)(4)

Option #2: Expulsion of Soviet Intelligence Personnel

US policy shall be to reduce the Soviet official personnel quota by the number of individuals expelled for espionage or

COPY 8 DE 17 COPIES
CIA

SECRET**SECRET**

SECRET

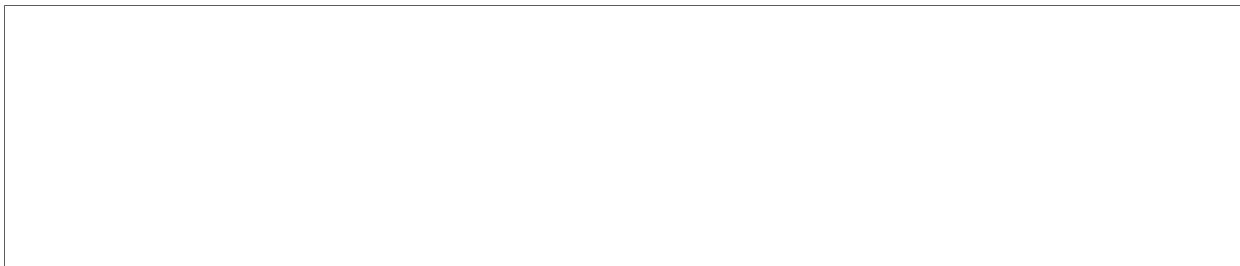
3

other intelligence-related activity. The Department of State shall give the Soviets notice that the US reserves the right to reduce the personnel ceiling of the Soviet Embassy and Consulate General by the number of persons expelled for espionage or other intelligence-related activity. Decisions on whether to expel personnel and/or reduce the personnel ceiling in specific cases shall be made by the Secretary of State or his designee, after consultation with the Department of Justice, and taking into consideration all relevant foreign policy and counter-intelligence factors. Implementation procedures for this option shall be developed by the CI/CM implementation task force. (S)

Option #3: Staffing of Proposed New York and Kiev Consulate

In negotiations with the Soviets concerning reopening of their consulate in New York City in return for a US Consulate in Kiev, agreements on manning of the two consulates will be consistent with the plan developed for Option #1. (S)

Option #4: Demarche to Peoples Republic of China



(b)(4)

Option #5: Increase Funding for INS Computer System

The Department of Justice and the Office of Management and Budget are to provide increased funding in the FY 1987 budget for the Immigration and Naturalization Service (INS) to expedite installation and operation of an INS computerized system to record more effectively arrivals, departures, and locations of foreign nationals visiting the US. (S)

Option #6: UN Secretariat Travel Through the OFM Service Bureau

United Nations Secretariat employees in New York City whose national missions to the United Nations are required to use the Office of Foreign Missions travel service bureau for both official and unofficial travel within the United States shall be also required to use that service bureau for all travel to the United States. (S)

COPY 8 OF 17 COPIES
CIA

SECRET**SECRET**

SECRET

4

Option #7: Require East European Officials to Arrange Travel Through the OFM Service Bureau

Require East European hostile country officials to use the OFM service bureau to book commercial transportation and public accommodations unless expressly waived in specific instances by the Secretary of State. (S)

Option #8: Close Areas of the US to East European Travel Following Espionage Activity

Place the East European allies of the Soviet Union on notice that areas of the United States now closed to travel for the Soviets may also be closed to them if any of their personnel are detected in espionage or intelligence-related activity in those areas. The decision to close an area shall be made by the Secretary of State in consultation with the Secretary of Defense, the Attorney General, and the Director of Central Intelligence. In the event the Secretary and Attorney General cannot agree, the NSC shall act as final arbiter. The closing of an area should be made on a selective basis, i.e., six months/one year, and should apply to the offending country officials only. (S)

Option #9: Close East European Commercial Offices Following Espionage Activity

Place the East European allies of the Soviet Union on notice that if a representative of their official commercial offices is detected in espionage or intelligence-related activity, that particular office may be closed. The decision to close the office shall be made by the Secretary of State, in consultation with the Attorney General. In the event the Secretary and Attorney General cannot agree, the NSC shall act as final arbiter. The Department of State shall test and/or expand legal authorities as necessary. (S)

Option #10: Controls on Foreign Corporations

Subject hostile country-owned/controlled corporations to the same controls and restrictions that the Office of Foreign Missions applies to the missions of foreign governments, to the extent authorized by the Foreign Missions Act. The Department of Justice and the FBI will study the activities of corporations individually and develop an implementation plan with immediate attention to be given those corporations presenting the greatest counterintelligence threat. The Department of Justice shall complete its study plan by December 31, 1985. (S)

COPY 8 OF 17 COPIES
CIA

SECRET**SECRET**

SECRET

SECRET

5

Option #11: Diplomatic Property Rights and Consolidated Offices

All legal means, including OFM authorities, other Federal, state, and local laws, as well as legislative initiatives, shall be employed to achieve the objective of controlling future hostile foreign government lease or ownership of real property within the US. The OFM shall work toward physical consolidation of the offices of Soviet as well as Soviet Bloc countries whenever feasible and legal. (S)

Option #12: Increase Denials of Soviet Military Attache Travel

Refuse travel requests by Soviet military attaches if their trips exceed those made by U.S. military attaches in the Soviet Union to enforce strict reciprocity. (S)

The task force should submit an initial report on the implementation of this NSDD no later than February 1, 1986. (U)

Ronald Reagan

COPY 8 OF 17 COPIES
CIA

SECRET

SECRET

E

THE WHITE HOUSE

WASHINGTON

SECRET/WITH CONFIDENTIAL ATTACHMENT

Executive Registry

84- 9216/1

September 17, 1984

MEMORANDUM FOR THE VICE PRESIDENT
 THE SECRETARY OF STATE
 THE SECRETARY OF THE TREASURY
 THE SECRETARY OF DEFENSE
 THE ATTORNEY GENERAL
 THE SECRETARY OF COMMERCE
 THE SECRETARY OF TRANSPORTATION
 THE SECRETARY OF ENERGY
 THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
 THE DIRECTOR OF CENTRAL INTELLIGENCE
 CHAIRMAN, JOINT CHIEFS OF STAFF
 ADMINISTRATOR, GENERAL SERVICES ADMINISTRATION
 DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
 DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY
 THE CHIEF OF STAFF, UNITED STATES ARMY
 THE CHIEF OF NAVAL OPERATIONS
 THE CHIEF OF STAFF, UNITED STATES AIR FORCE
 COMMANDANT, UNITED STATES MARINE CORPS
 DIRECTOR, DEFENSE INTELLIGENCE AGENCY
 DIRECTOR, NATIONAL SECURITY AGENCY
 MANAGER, NATIONAL COMMUNICATIONS SYSTEM

SUBJECT: National Policy on Telecommunications and
 Automated Information Systems Security (U)

The President has approved and signed the attached National Security Decision Directive which establishes initial national objectives, policies and an improved organizational structure for protecting US telecommunications and automated information systems from exploitation by hostile intelligence activities. (U)

The Secretary of Defense's recent biennial report to the President on the security of US Government communications concludes that when viewed from a national perspective, the security of our communications is perilous and that intelligence available to hostile intelligence services through unprotected or inadequately protected US communications is unsurpassed for its timeliness, accuracy, completeness and affects every aspect of our national security. This NSDD establishes a means by which the government can develop measures to adequately secure our communications. (S)

SECRET/WITH CONFIDENTIAL ATTACHMENTCOPY 11 OF 22 COPIES
CIA

Declassify on: OADR

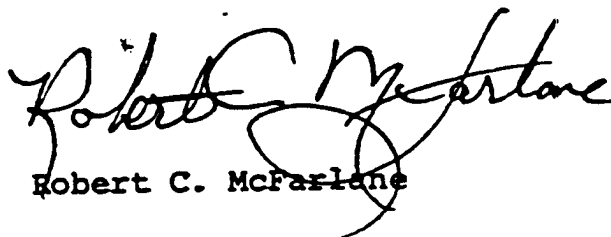
SECRET

SECRET/WITH CONFIDENTIAL ATTACHMENT

In order to begin this vital task, the Chairman of the National Communications Security Committee (NCSC) is requested to immediately expand the NCSC into the new National Telecommunications and Information Systems Security Committee (NTISSC) and prepare an initial plan for implementation of the NSDD for submission to the steering group by October 1, 1984. (U)

Authority for distributing additional copies of the NSDD to appropriate agencies throughout the government will be provided to the Chairman of the NTISSC and the Manager, National Communications Systems, in the near future. (U)

FOR THE PRESIDENT:


Robert C. McFarlane

Attachment
National Security
Decision Directive 145

SECRET/WITH CONFIDENTIAL ATTACHMENT

COPY 11 OF 22 COPIES

~~CONFIDENTIAL~~

THE WHITE HOUSE

WASHINGTON

September 17, 1984

Executive Registry

84- 9216

CONFIDENTIAL

*National Security Decision
Directive Number 145*

NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY (U)

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation. (U)

Within the government these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities. (U)

This Directive: Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns

CONFIDENTIAL

~~CONFIDENTIAL~~

COPY 11 OF 22 COPIES

responsibilities for implementation. It is intended to assure full participation and cooperation among the various existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat to these systems, and to foster an appropriate partnership between government and the private sector in attaining these goals. This Directive specifically recognizes the special requirements for protection of intelligence sources and methods. It is intended that the mechanisms established by this Directive will initially focus on those automated information systems which are connected to telecommunications transmission systems. (U)

I. Objectives. Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector information are key national responsibilities. I, therefore, direct that the government's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained or improved to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and support for a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government resources and encouragement of private sector security initiatives.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems. (U)

2. Policies. In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secured by such means as are necessary to prevent compromise or exploitation.

b. Systems handling other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest,

CONFIDENTIAL

CONFIDENTIAL

COPY # DE 22 COPIES

shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

c. The government shall encourage, advise, and, where appropriate, assist the private sector to: identify systems which handle sensitive non-government information, the loss of which could adversely affect the national security; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national security interest, the private sector shall be encouraged, advised, and, where appropriate, assisted in undertaking the application of such measures.

d. Efforts and programs begun under PD-24 which support these policies shall be continued. (U)

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies. (U)

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the Executive Agent and through him to the National Manager with respect to the activities undertaken to implement this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of those telecommunications and automated information systems that handle classified or sensitive government or government-derived information with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

CONFIDENTIAL

COPY 11 OF 22 COPIES

(4) Review consolidated resources program and budget proposals for telecommunications systems security, including the COMSEC Resources Program, for the US Government and provide recommendations to OMB for the normal budget review process.

(5) Review in aggregate the program and budget proposals for the security of automated information systems of the departments and agencies of the government.

(6) Review and approve matters referred to it by the Executive Agent in fulfilling the responsibilities outlined in paragraph 6. below.

(7) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(8) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(9) Recommend for Presidential approval additions or revisions to this Directive as national interests may require.

(10) Identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information. (U)

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group. (U)

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be composed of a voting representative of each member of the Steering Group and of each of the following:

The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy

CONFIDENTIAL

COPY 11 OF 22 COPIES

Chairman, Joint Chiefs of Staff
Administrator, General Services Administration
Director, Federal Bureau of Investigation
Director, Federal Emergency Management Agency
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
Commandant, United States Marine Corps
Director, Defense Intelligence Agency
Director, National Security Agency
Manager, National Communications System (U)

b. The Committee shall:

(1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Provide telecommunication and automated information systems security guidance to the departments and agencies of the government.

(3) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.

(4) Identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures.

(5) Approve the release of sensitive systems technical security material, information, and techniques to foreign governments or international organizations with the concurrence of the Director of Central Intelligence for those activities which he manages.

(6) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.

(7) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.

(8) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

(9) Interact with the National Communications System Committee of Principals established by Executive Order

CONFIDENTIAL

12472 to ensure the coordinated execution of assigned responsibilities. (U)

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on automated information systems security. The two subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate, while considering any differences in the level of maturity of the technologies to support such implementation. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important. (U)

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency shall provide facilities and support as required. Other departments and agencies shall provide facilities and support as requested by the Chairman. (U)

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Automated Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures.

b. Procure for and provide to departments and agencies of the government and, where appropriate, to private institutions (including government contractors) and foreign governments, technical security material, other technical assistance, and other related services of common concern, as required to accomplish the objectives of this Directive.

c. Approve and provide minimum security standards and doctrine, consistent with provisions of the Directive.

d. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

CONFIDENTIAL

CONFIDENTIAL

COPY 11 OF 22 COPIES

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Review and assess for the Steering Group the proposed telecommunications systems security programs and budgets for the departments and agencies of the government for each fiscal year and recommend alternatives, where appropriate. The views of all affected departments and agencies shall be fully expressed to the Steering Group.

g. Review for the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for each fiscal year. (U)

7. The National Manager for Telecommunications Security and Automated Information Systems Security. The Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall have authority in the name of the Executive Agent to:

a. Examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Orders and applicable Presidential Directives. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned.

b. Act as the government focal point for cryptography, telecommunications systems security, and automated information systems security.

c. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

d. Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

e. Conduct foreign communications security liaison, including agreements with foreign governments and with international and private organizations for telecommunications and automated information systems security, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Agreements shall be coordinated with affected departments and agencies.

CONFIDENTIAL

CONFIDENTIAL

COPY 11 OF 22 PAGES

f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other technical security material or services.

g. Assess the overall security posture and disseminate information on hostile threats to telecommunications and automated information systems security.

h. Operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems.

i. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

j. Review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the government, and recommend alternatives, where appropriate, for the Executive Agent and the Steering Group.

k. Review annually the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for the Executive Agent and the Steering Group.

l. Request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein.

m. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including government contractors, and foreign governments. (U)

8. The Heads of Federal Departments and Agencies shall:

a. Be responsible for achieving and maintaining a secure posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential Directives. (U)

CONFIDENTIAL

CONFIDENTIAL

COPY // OF 22 COPIES

9. Additional Responsibilities.

a. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use such Federal Information Processing Standards for the security of information in automated information systems as the Steering Group may approve. The Manager, National Communications System, through the Administrator, General Services Administration, shall develop and issue for public use such Federal Telecommunications Standards for the security of information in telecommunications systems as the National Manager may approve. Such standards, while legally applicable only to Federal Departments and Agencies, shall be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector.

b. The Director, Office of Management and Budget, shall:

(1) Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to telecommunications systems security and automated information systems security of the departments and agencies of the government.

(2) Consolidate and provide such data to the National Manager via the Executive Agent.

(3) Review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein. (U)

10. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Executive Agent, or the National Manager authority to examine the facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein.

c. Amends or contravenes the provisions of existing law, Executive Orders, or Presidential Directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

CONFIDENTIAL

CONFIDENTIAL

COPY 11 OF 22 COPIES

d. Is intended to establish additional review processes for the procurement of automated information processing systems. (U)

11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information.

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information systems. (U)

12. The Interagency Committee on Real Estate Acquisitions (ICREA) in the United States established under PD-24 shall be reconstituted under the chairmanship of the Director, Office of Foreign Missions, Department of State, with representation from the Department of Defense, the Department of Justice/Federal Bureau of Investigation, the Director of Central Intelligence, the National Security Agency, and the Assistant to the President for National Security Affairs. The Committee, with advice from the Reciprocity Policy Committee of the Department of State, shall provide policy guidance for implementation by the Office of Foreign Missions or other appropriate organizations, on proposals for foreign real estate acquisitions by lease or purchase, that present a threat to US telecommunications and automated information systems security

[Redacted]

(C)

[Redacted]

13. The functions of the Interagency Group for Telecommunications Protection and the National Communications

25X1
25X1

Security Committee (NCSC) as established under PD-24 are subsumed by the Systems Security Steering Group and the NTISSC, respectively. The policies established under the authority of the Interagency Group or the NCSC; which have not been superseded by this Directive, shall remain in effect until modified or rescinded by the Steering Group or the NTISSC, respectively. (U)

14. Except for ongoing telecommunications protection activities mandated by and pursuant to PD/NSC-24, that Directive is hereby superseded and cancelled. (U)

Ronald Reagan

CONFIDENTIAL

CONFIDENTIAL

COPY 11 OF 22 COPIES

F

SECRET

Interagency Group/Countermeasures

Washington, D.C. 20505

D/ICS-85-7671
27 September 1985

MEMORANDUM FOR: Members and Invitees

FROM: [Redacted]
Acting Executive Secretary

25X1:1

SUBJECT: Final Minutes—16th IG/CM Meeting, 21 August 1985

Attached are final minutes of the 16th IG/CM meeting held on 21 August

1985. [Redacted]

25X1

25X1

25X1

Attachment:
a/s

Regrade Unclassified when separated
from classified attachment.

25X1

SECRET

Page Denied

Next 6 Page(s) In Document Denied

CONFIDENTIAL

ATTACHMENT 1

ATTENDEES
IG/CM MEETING, 21 AUGUST 1985

NAME

ALDERMAN, Craig
SNIDER, L. Britt
DONNELLY, John F.
WORTZEL, Larry



CALLO, Anthony
GUENTHER, John
PORTER, Harry



LAWTON, Mary C.
ALLEN, Robert C.
LUNDSTROM, Edward
PASEUR, George
GARFINKEL, Steven
MAJOR, David
JACKSON, Byron
VAN TUYL, Robert M., Jr.



ORGANIZATION

OSD

OSD

OSD

OSD

DIA

NSA

Army

Marine Corps

FBI

CIA

CIA

Justice

Navy

State

Air Force

ISOO

NSC

Commerce

Commerce

SECOM

CCIS/ICS

CCIS/ICS

25X1

25X1

25X1

CONFIDENTIAL

Page Denied

Next 11 Page(s) In Document Denied

ATTENDEES

<u>NAME</u>	<u>ORGANIZATION</u>
POLLARI, Ray	OSD
TAYLOR, Frank	OSD
[REDACTED]	NSA
	NSA
	NSA
	NSA
	Army
	Army
	Navy
GALLO, Anthony	Air Force
McCULLAH, Lanny	Marine Corps
LAW, Richard F.	Marine Corps
GUENTHER, John	FBI
ROBINSON, Lloyd A.	FBI
GEER, James H.	CIA
DuHADWAY, Thomas	NSC
[REDACTED]	Justice
MAJOR, David G.	Justice
LAWTON, Mary C.	DIA
ALLAN, Kimberly	State
[REDACTED]	State
HEICHLER, Lucian	State
HARDESTY, Linda	State
SHEAR, David	State
O'BRIEN, Patrick O.	Energy
O'BRIEN, Robert	Energy
RITCHIE, Louis	ICS
[REDACTED]	ICS
	ICS
	ICS

25X1:1

25X1:1

25X1:1

25X1

CONFIDENTIAL

Page Denied

H

Page Denied

Next 3 Page(s) In Document Denied

CONFIDENTIAL

ATTENDEES

MEMBERS

David G. Major, Chairman
Robert E. Lamb

[Redacted]

John F. Donnelly

[Redacted]

Thomas DuHadway
James Nolan

[Redacted]

OBSERVERS

Douglas Mulholland
Ronald L. Fann
Lance Arnold
Leon Banker

[Redacted]

ORGANIZATION

NSC
State
CIA
CIA
OSD
DIA (for JCS)
FBI
OFM
ICS
ICS

25X1

25X1

25X1

ORGANIZATION

Treasury
Army
Navy
Air Force
NSA
NSA
CIA

25X1

CONFIDENTIAL

Page Denied

Next 2 Page(s) In Document Denied