



Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4

OFFICE OF MANAGEMENT AND BUDGET

WASHINGTON, D.C. 20503

July 27, 1978

CIRCULAR NO. A-71  
Transmittal Memorandum No. 1

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Security of Federal automated information systems

1. Purpose. This Transmittal Memorandum to OMB Circular No. A-71 dated March 6, 1965 promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies. More specifically, it:

a. Defines the division of responsibility for computer security between line operating agencies and the Department of Commerce, the General Services Administration, and the Civil Service Commission.

b. Establishes requirements for the development of management controls to safeguard personal, proprietary and other sensitive data in automated systems.

c. Establishes a requirement for agencies to implement a computer security program and defines a minimum set of controls to be incorporated into each agency computer security program.

d. Requires the Department of Commerce to develop and issue computer security standards and guidelines.

e. Requires the General Services Administration to issue policies and regulations for the physical security of computer rooms consistent with standards and guidelines issued by the Department of Commerce; assure that agency procurement requests for automated data processing equipment, software, and related services include security requirements; and assure that all procurements made by GSA meet the security requirements established by the user agency.

f. Requires the Civil Service Commission to establish personnel security policies for Federal personnel associated

(No. A-71)

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4  
with the design, operation or maintenance of Federal computer systems, or having access to data in Federal computer systems.

2. Background. Increasing use of computer and communications technology to improve the effectiveness of governmental programs has introduced a variety of new management problems. Many public concerns have been raised in regard to the risks associated with automated processing of personal, proprietary or other sensitive data. Problems have been encountered in the misuse of computer and communications technology to perpetrate crime. In other cases, inadequate administrative practices along with poorly designed computer systems have resulted in improper payments, unnecessary purchases or other improper actions. The policies and responsibilities for computer security established by this Transmittal Memorandum supplement policies currently contained in OMB Circular No. A-71.

3. Definitions. The following definitions apply for the purposes of this memorandum:

a. "Automated decisionmaking systems" are computer applications which issue checks, requisition supplies or perform similar functions based on programmed criteria, with little human intervention.

b. "Contingency plans" are plans for emergency response, back-up operations and post-disaster recovery.

c. "Security specifications" are a detailed description of the safeguards required to protect a sensitive computer application.

d. "Sensitive application" is a computer application which requires a degree of protection because it processes sensitive data or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application (e.g., automated decisionmaking systems).

e. "Sensitive data" is data which requires a degree of protection due to the risk and magnitude of loss or harm which could result from inadvertent or deliberate disclosure, alteration, or destruction of the data (e.g., personal data, proprietary data).

4. Responsibility of the heads of executive agencies. The head of each executive branch department and agency is

(No. A-71)

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4  
responsible for assuring an adequate level of security for all agency data whether processed in-house or commercially. This includes responsibility for the establishment of physical, administrative and technical safeguards required to adequately protect personal, proprietary or other sensitive data not subject to national security regulations, as well as national security data. It also includes responsibility for assuring that automated processes operate effectively and accurately. In fulfilling this responsibility each agency head shall establish policies and procedures and assign responsibility for the development, implementation, and operation of an agency computer security program. The agency's computer security program shall be consistent with all Federal policies, procedures and standards issued by the Office of Management and Budget, the General Services Administration, the Department of Commerce, and the Civil Service Commission. In consideration of problems which have been identified in relation to existing practices, each agency's computer security program shall at a minimum:

a. Assign responsibility for the security of each computer installation operated by the agency, including installations operated directly by or on behalf of the agency (e.g., government-owned contractor operated facilities), to a management official knowledgeable in data processing and security matters.

b. Establish personnel security policies for screening all individuals participating in the design, operation or maintenance of Federal computer systems or having access to data in Federal computer systems. The level of screening required by these policies should vary from minimal checks to full background investigations commensurate with the sensitivity of the data to be handled and the risk and magnitude of loss or harm that could be caused by the individual. These policies should be established for government and contractor personnel. Personnel security policies for Federal employees shall be consistent with policies issued by the Civil Service Commission.

c. Establish a management control process to assure that appropriate administrative, physical and technical safeguards are incorporated into all new computer applications and significant modifications to existing computer applications. This control process should evaluate the sensitivity of each application. For sensitive applications, particularly those which will process sensitive data or which will have a high potential for loss,

(No. A-71)

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4

such as automated decisionmaking systems, specific controls should, at a minimum, include policies and responsibilities for:

(1) Defining and approving security specifications prior to programming the applications or changes. The views and recommendations of the computer user organization, the computer installation and the individual responsible for the security of the computer installation shall be sought and considered prior to the approval of the security specifications for the application.

(2) Conducting and approving design reviews and application systems tests prior to using the systems operationally. The objective of the design reviews should be to ascertain that the proposed design meets the approved security specifications. The objective of the system tests should be to verify that the planned administrative, physical and technical security requirements are operationally adequate prior to the use of the system. The results of the design review and system test shall be fully documented and maintained as a part of the official records of the agency. Upon completion of the system test, an official of the agency shall certify that the system meets the documented and approved system security specifications, meets all applicable Federal policies, regulations and standards, and that the results of the test demonstrate that the security provisions are adequate for the application.

d. Establish an agency program for conducting periodic audits or evaluations and recertifying the adequacy of the security safeguards of each operational sensitive application including those which process personal, proprietary or other sensitive data, or which have a high potential for financial loss, such as automated decisionmaking applications. Audits or evaluations are to be conducted by an organization independent of the user organization and computer facility manager. Recertifications should be fully documented and maintained as a part of the official documents of the agency. Audits or evaluations and recertifications shall be performed at time intervals determined by the agency, commensurate with the sensitivity of information processed and the risk and magnitude of loss or harm that could result from the application operating improperly, but shall be conducted at least every three years.

e. Establish policies and responsibilities to assure that appropriate security requirements are included in

(No. A-71)

specifications for the acquisition or operation of computer facilities, equipment, software packages, or related services, whether procured by the agency or by the General Services Administration. These requirements shall be reviewed and approved by the management official assigned responsibility for security of the computer installation to be used. This individual must certify that the security requirements specified are reasonably sufficient for the intended application and that they comply with current Federal computer security policies, procedures, standards and guidelines.

f. Assign responsibility for the conduct of periodic risk analyses for each computer installation operated by the agency, including installations operated directly by or on behalf of the agency. The objective of this risk analysis should be to provide a measure of the relative vulnerabilities at the installation so that security resources can effectively be distributed to minimize the potential loss. A risk analysis shall be performed:

(1) Prior to the approval of design specifications for new computer installations.

(2) Whenever there is a significant change to the physical facility, hardware or software at a computer installation. Agency criteria for defining significant changes shall be commensurate with the sensitivity of the information processed by the installation.

(3) At periodic intervals of time established by the agency, commensurate with the sensitivity of the information processed by the installation, but not to exceed five years, if no risk analysis has been performed during that time.

g. Establish policies and responsibilities to assure that appropriate contingency plans are developed and maintained. The objective of these plans should be to provide reasonable continuity of data processing support should events occur which prevent normal operations. These plans should be reviewed and tested at periodic intervals of time commensurate with the risk and magnitude of loss or harm which could result from disruption of data processing support.

5. Responsibility of the Department of Commerce. The Secretary of Commerce shall develop and issue standards and

(No. A-71)

guidelines for assuring security of automated information. Each standard shall, at a minimum, identify:

- a. Whether the standard is mandatory or voluntary.
- b. Specific implementation actions which agencies are required to take.
- c. The time at which implementation is required.
- d. A process for monitoring implementation of each standard and evaluating its use.
- e. The procedure for agencies to obtain a waiver to the standard and the conditions or criteria under which it may be granted.

6. Responsibility of the General Services Administration.  
The Administrator of General Services shall:

- a. Issue policies and regulations for the physical security of computer rooms in Federal buildings consistent with standards and guidelines issued by the Department of Commerce.

- b. Assure that agency procurement requests for computers, software packages, and related services include security requirements which have been certified by a responsible agency official. Delegations of procurement authority to agencies by the General Services Administration under mandatory programs, dollar threshold delegations, certification programs or other so-called blanket delegations shall include requirements for agency specifications and agency certification of security requirements. Other delegations of procurement authority shall require specific agency certification of security requirements as a part of the agency request for delegation of procurement authority.

- c. Assure that specifications for computer hardware, software, related services or the construction of computer facilities are consistent with standards and guidelines established by the Secretary of Commerce.

- d. Assure that computer equipment, software, computer room construction, guard or custodial services, telecommunications services, and any other related services procured by the General Services Administration meet the security requirements established by the user agency and are

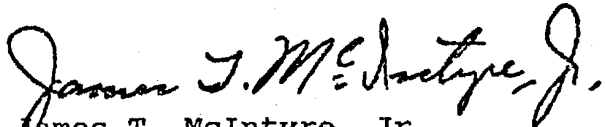
(No. A-71)

consistent with other applicable policies and standards issued by OMB, the Civil Service Commission and the Department of Commerce. Computer equipment, software, or related ADP services acquired by the General Services Administration in anticipation of future agency requirements shall include security safeguards which are consistent with mandatory standards established by the Secretary of Commerce.

7. Responsibility of the Civil Service Commission. The Chairman of the Civil Service Commission shall establish personnel security policies for Federal personnel associated with the design, operation or maintenance of Federal computer systems, or having access to data in Federal computer systems. These policies should emphasize personnel requirements to adequately protect personal, proprietary or other sensitive data as well as other sensitive applications not subject to national security regulations. Requirements for personnel checks imposed by these policies should vary commensurate with the sensitivity of the data to be handled and the risk and magnitude of loss or harm that could be caused by the individual. The checks may range from merely normal reemployment screening procedures to full background investigations.

8. Reports. Within 60 days of the issuance of this Transmittal Memorandum, the Department of Commerce, General Services Administration and Civil Service Commission shall submit to OMB plans and associated resource estimates for fulfilling the responsibilities specifically assigned in this memorandum. Within 120 days of the issuance of this Transmittal Memorandum, each executive branch department and agency shall submit to OMB plans and associated resource estimates for implementing a security program consistent with the policies specified herein.

9. Inquiries. Questions regarding this memorandum should be addressed to the Information Systems Policy Division (202) 395-4814.

  
James T. McIntyre, Jr.  
Director

(No. A-71)

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4

preservation, and facilitate the segregation and disposal of records of temporary value, and (3) compliance with the provisions of sections 392-396, 397-401 of this title and the regulations issued thereunder.

(c) Storage, processing, and servicing of records.

Whenever the head of a Federal agency determines that substantial economies or increased operating efficiency can be effected thereby, he shall provide for the storage, processing, and servicing of records that are appropriate therefor in a records center maintained and operated by the Administrator or, when approved by the Administrator, in such a center maintained and operated by the head of such Federal agency.

(d) Certifications and determinations on transferred records.

Any official of the Government who is authorized to certify to facts on the basis of records in his custody, is authorized to certify to facts on the basis of records that have been transferred by him or his predecessors to the Administrator, and may authorize the Administrator to certify to facts and to make administrative determinations on the basis of records transferred to the Administrator, notwithstanding any other provisions of law.

(e) Safeguards.

The head of each Federal agency shall establish such safeguards against the removal or loss of records as he shall determine to be necessary and as may be required by regulations of the Administrator. Such safeguards shall include making it known to all officials and employees of the agency (1) that no records in the custody of the agency are to be alienated or destroyed except in accordance with the provisions of sections 366-376 and 378-380 of this title, and (2) the penalties provided by law for the unlawful removal or destruction of records.

(f) Unlawful removal, destruction, etc.

The head of each Federal agency shall notify the Administrator of any actual, impending, or threatened unlawful removal, defacing, alteration, or destruction of records in the custody of the agency of which he is the head that shall come to his attention, and with the assistance of the Administrator shall institute action through the Attorney General for the recovery of records he knows or has reason to believe have been unlawfully removed from his agency, or from any other Federal agency whose records have been transferred to his legal custody.

(g) Authority of Comptroller General.

Nothing in sections 392-396, 397-401 of this title shall be construed as limiting the authority of the Comptroller General of the United States with respect to prescribing accounting systems, forms, and procedures, or lessening the responsibility of collecting and disbursing officers for rendition of their accounts for settlement by the General Accounting Office. (June 30, 1949, ch. 238, title V, § 506, as added Sept. 5, 1950, ch. 849, § 6 (d), 61 Stat. 583, and amended Feb. 5, 1964, Pub. L. 88-275, 78 Stat. 8.)

AMENDMENTS

1964-Subsec. (d) Pub. L. 88-275 provides authorization for Administrator to certify facts and make administrative determinations based on transferred records.

§ 396a. Final authority of Administrator in matters regarding surveys of records, etc.

Notwithstanding any other provision of the Federal Property and Administrative Services Act of 1949, as amended, the Administrator shall have final authority in all matters involving the conduct of surveys of Government records, and records creation, maintenance, management and disposal practices in Federal agencies, pursuant to sections 395 and 396 of this title, and the implementation of recommendations based on such surveys. (Aug. 26, 1954, ch. 935, ch. XIII, § 801, 68 Stat. 816.)

REFERENCE IN TEXT

The Federal Property and Administrative Services Act of 1949, as amended, referred to in the text of this section, is classified to this chapter, chapter 110 of Title 5, Executive Department, and Government Officers and Employees, chapter 13 of Title 40, Public Buildings, Property and Works, and section 5 of chapter 1 of Title 41, Public Contracts.

CODIFICATION

Section was enacted as a part of the Supplemental Appropriation Act, 1950, and not as a part of the Federal Property and Administrative Services Act of 1949, part of which comprised this chapter of the Federal Records Act of 1950, which is a part of the Federal Property and Administrative Services Act of 1949, and which is classified to sections 392-396 and 397-401 of this title (see references in text made above). Codification note under section 391 of this title, and Stat. Title note under section 392 of this title.

§ 397. Archival administration.

(a) Acceptance of records for historical preservation. The Administrator, whenever it appears to him to be in the public interest, is authorized—

(1) to accept for deposit with the National Archives of the United States the records of any Federal agency or of the Congress of the United States that are determined by the Archivist to have sufficient historical or other value to warrant their continued preservation by the United States Government.

(2) to direct and effect the transfer to the National Archives of the United States of any records of any Federal agency that have been in existence for more than fifty years and that are determined by the Archivist to have sufficient historical or other value to warrant their continued preservation by the United States Government, unless the head of the agency which has custody of them shall certify in writing to the Administrator that they must be retained in his custody for use in the conduct of the regular current business of the said agency.

(3) to direct and effect, with the approval of the head of the originating agency (or if the existence of such agency shall have been terminated, then with the approval of his successor in function if any), the transfer of records deposited (or approved for deposit) with the National Archives of the United States to public or educational institution or associations: *Provided*, That the title to such records shall remain vested in the United States unless otherwise authorized by Congress; and

(4) to direct and effect the transfer of materials from private sources authorized to be received



**ILLEGIB**

**Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4**

**Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4**

***BEST COPY***  
***AVAILABLE***

STAT

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4

Next 97 Page(s) In Document Exempt

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4

**DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/7<sup>1</sup>**  
**CONTROL OF DISSEMINATION OF FOREIGN INTELLIGENCE**

(Effective 18 May 1976)

Pursuant to Section 102 of the National Security Act of 1947, Executive Order 11905 and National Security Council Intelligence Directives, certain controls on dissemination of foreign intelligence and related material<sup>2</sup> (hereafter referred to as foreign intelligence) are hereby established and promulgated.

**1. Purpose**

This directive establishes certain common controls and procedures for the use and dissemination of foreign intelligence to ensure that, while facilitating the interchange of information for intelligence purposes, there will be adequate protection of foreign intelligence sources and methods. This directive restates applicable portions of National Security Council Directive of 17 May 1972 implementing Executive Order 11652, and prescribes additional controls applicable to the US foreign intelligence mission. The policy on release of foreign intelligence to contractors is set forth in the Attachment.

**2. Applicability**

The controls and procedures set forth in this directive shall be uniformly applied within the Executive Branch of the Government in handling of all materials containing foreign intelligence originated by Intelligence Community organizations as defined by Section 2(b) of Executive Order 11905.

**3. National Security Council Directive**

a. National Security Council Directive of 17 May 1972 implementing Executive Order 11652 stipulates that, except as otherwise provided by Section 102 of the National Security Act of 1947, classified information or material originating in one department shall not be disseminated outside any other department to which it has been made available without the consent of the originating department. This restriction on dissemination is commonly described as the "third agency rule."

b. The NSC Directive stipulates that the dissemination of classified information, including intelligence and intelligence information, orally,

<sup>1</sup>This directive supersedes DCID No. 1/7 effective 5 October 1975.

<sup>2</sup>For purposes of this directive, "related material" includes: information describing US foreign intelligence sources and methods, equipment and methodology unique to the acquisition or exploitation of foreign intelligence, foreign military hardware obtained for exploitation and photography or recordings resulting from US foreign intelligence collection efforts.

in writing or by any other means, shall be limited to those persons whose official duties or contractual obligations require knowledge or possession of such information and its dissemination to those persons.

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4

c. The NSC Directive also states that documents or portions of documents containing TOP SECRET information shall not be reproduced without the consent of the originating office. All other classified material shall be reproduced sparingly and any stated prohibition against reproduction shall be strictly adhered to.

d. The NSC Directive further requires that the marking, "WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED," be prominently displayed on all information and materials relating to sensitive intelligence sources and methods; and, that materials so marked will not be disseminated in any manner outside authorized channels without the permission of the originating department and an assessment by the senior intelligence official in the disseminating department as to the potential risk to the national security and to the intelligence sources and methods involved.<sup>3</sup> For special purposes, primarily bibliographic notation, communications or automatic data processing, this marking may be abbreviated WNINTEL.

#### 4. Advance authorization

a. To facilitate the dissemination and different uses made of classified foreign intelligence within and among Intelligence Community organizations and to assure the timely provision of intelligence to consumers and to handle the volume of such materials in a practical way, it is necessary to provide controlled relief to the "third agency rule" within the Intelligence Community in addition to that provided by Section 102 of the National Security Act of 1947. Accordingly, Intelligence Community organizations have been given advance authorization to use each other's classified foreign intelligence in their respective intelligence documents, publications or other information media, and to disseminate their products to third agencies or foreign governments,<sup>4</sup> subject to limitations and procedures prescribed in this directive.

b. Classified foreign intelligence documents, even though they bear no control markings, will not be released in their original form to third agencies or foreign governments without permission of the originator. Information contained in classified foreign intelligence documents of another organization may be extracted or paraphrased and used by the recipient Intelligence Community organization in classified foreign intelligence reports and released to third agencies, except as specifically restricted by control

<sup>3</sup> Unless otherwise specified by the Director of Central Intelligence in consultation with the National Foreign Intelligence Board or as agreed to between originating and recipient agencies, authorized channels include Intelligence Community organizations and within each organization (including their contractors and consultants) as determined by the recipient senior intelligence official.

<sup>4</sup> Excepting RESTRICTED DATA and formerly RESTRICTED DATA, which is prohibited from foreign dissemination under Sections 123 and 144 of Public Law 585, Atomic Energy Act of 1954, as amended.

markings prescribed in this directive. For purposes of this authorization, "WARNING NOTICE SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" shall not be considered a restrictive marking.

c. Information contained in classified foreign intelligence documents of another organization not bearing any control markings may be extracted or paraphrased and used by the recipient Intelligence Community organization in reports disseminated to foreign governments provided:<sup>5</sup>

(1) No reference is made to the source documents upon which the released product is based.

(2) The source and manner of acquisition of the information are not revealed.

(3) Foreign release is made through established foreign disclosure channels and procedures.

d. Any organization disseminating foreign intelligence beyond the organizations of the Intelligence Community shall be responsible for ensuring that recipient organizations understand and agree to observe the restrictions prescribed by this directive and maintain adequate safeguards.

e. No release of a classified foreign intelligence document, whether or not bearing a control marking, shall be made to foreign nationals and immigrant aliens, including US Government employed, utilized or integrated foreign nationals and immigrant aliens, without the permission of the originating agency.

##### 5. *Additional authorized control markings*

a. In addition to the WARNING NOTICE prescribed by NSC Directive, any of the following additional markings may be used on foreign intelligence whenever, in the opinion of the originating organization, extraordinary circumstances related to the intelligence source or method require more specific dissemination restrictions. Use of these markings shall be limited to foreign intelligence, the disclosure of which, could: compromise the status of collaborating foreign governments or officials or otherwise seriously damage US relations with foreign governments; subject US citizens or others to the possibility of personal danger or incarceration; seriously impair the continuing cooperation of private individuals providing foreign intelligence; seriously affect the continuing viability of vital technical collection programs; or, result in the possible compromise or loss of some unique foreign intelligence source or method. These control markings will be individually assigned at the time of preparation of the completed document and used in conjunction with classification and other markings required by Executive Order 11652 and the implementing NSC Directive and, unless otherwise indicated in 6a below, carried forward to any new format in which that information is incorporated, including oral and visual presentations.

<sup>5</sup> See footnote 4, paragraph 4a.

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4  
(1) "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR"

This marking shall be used when unique source sensitivity factors, known to the originator, require strict compliance with third agency rule procedures, in addition to a continuing knowledge and supervision on the part of the originator as to the extent to which the original document and information contained therein is disseminated. Documents and information bearing this marking will not be disseminated beyond the Headquarters elements of the recipient organizations and the information contained therein shall not be extracted and incorporated into other reports without the permission of and under conditions prescribed by the originator. (For special purposes, primarily bibliographic notation, communications and automatic data processing, this marking may be abbreviated ORCON.)

(2) "NFIB DEPARTMENTS ONLY"

Foreign intelligence so marked will not be disseminated to organizations not represented on the National Foreign Intelligence Board without the permission of the originating agency. Within each National Foreign Intelligence Board organization dissemination shall be as determined by the recipient senior intelligence official, and may include organization contractors and consultants unless specifically prohibited by addition of the "NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS" marking described below. (For special purposes, primarily bibliographic notation, communications and automatic data processing, this marking may be abbreviated NFIBONLY.)

(3) "NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS"

Foreign intelligence so marked shall not be disseminated to contractors or contractor consultants without the permission of the originating agency. Examples of when this marking may be used include National Intelligence Estimates and similar national intelligence reports and other foreign intelligence, which, if disseminated to consultants or contractors, might seriously impair the continuing cooperation of contributing private individuals. This restriction shall not apply to those consultants hired under Civil Service Commission procedures, or comparable procedures derived from authorities vested in heads of organizations by law, and who are normally considered an extension of the office by which they are employed. In applying this control marking, originators will give consideration to the need of Intelligence Community organizations to use contractor consultants and contractors to perform services which cannot be adequately performed by US Government personnel. (For special purposes, primarily bibliographic notation, communications and automatic data processing, this marking may be abbreviated NOCONTRACT.)

(4) "CAUTION—PROPRIETARY INFORMATION INVOLVED"

This marking will be used in conjunction with foreign intelligence obtained from various sources in the US private business sector, and as the information may bear upon proprietary interests of the source, or may

otherwise be used to the sources' detriment. Recipients of reports bearing this marking shall take every reasonable precaution to ensure that the information is not used to the detriment of the source. This marking may be used in conjunction with the "NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS" marking described above. (For special purposes, primarily bibliographic notation, communications and automatic data processing, this marking may be abbreviated PROPIN.)

(5) "NOT RELEASABLE TO FOREIGN NATIONALS"

Foreign intelligence so marked involves special considerations requiring that it not be released in any form to foreign governments, foreign nationals or non-US citizens without the permission of the originating agency. Examples of when this control marking may be used include: the possible compromise of the status of relations with collaborating foreign governments, or officials; or jeopardizing the continuing viability of vital technical collection programs. (For special purposes, primarily bibliographic notation, communications and automatic data processing, this marking may be abbreviated NOFORN.) When the originating agency predetermines that information can be released to a specified foreign government(s), the following marking may be used: "THIS INFORMATION HAS BEEN AUTHORIZED FOR RELEASE TO (specified country(s))." (For special purposes, primarily bibliographic notation, communications and automatic data processing, this marking may be abbreviated "REL (specified country(s)).")

6. *Procedures governing use of control markings*

a. Any recipient desiring to use foreign intelligence in a manner contrary to the restrictions established by the control markings set forth above shall obtain the permission of the originating agency. Such permission applies only to the specific purpose agreed to by the originator and does not automatically apply to all recipients of the information as originally disseminated unless the originating agency removes the control markings for the benefit of the recipients. In those cases where dissemination outside the recipient agency is desired utilizing lesser or no control markings, the recipient agency should prepare a sanitized version which may be released with the originator's permission.

b. Control markings authorized in paragraphs 3d and 5 above, shall be displayed prominently on documents, incorporated in the text of communication messages, and associated with data stored or processed in automatic data processing systems. Unless the entire document justifies the protection of the control marking(s), each portion requiring the marking(s) shall, to the extent feasible, be marked with the appropriate marking abbreviation authorized by this directive.

c. The standardized restrictions and control markings set forth in this directive are to be employed uniformly by all organizations in the Intelligence Community, thereby assuring like control and restrictions on the use of foreign intelligence disseminated within the organizations represented on the National Foreign Intelligence Board.



Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4

d. The substance of this directive shall be published in appropriate regulatory or notice media of each organization, together with appropriate procedures permitting rapid interagency consultation. Each Intelligence Community organization will designate a primary referent.

7. *Report of unauthorized disclosure*

Violations of the foregoing restrictions and control markings that result in unauthorized disclosure by one agency of the foreign intelligence of another shall be reported to the Director of Central Intelligence through the DCI Security Committee.

8. *Prior restrictions and markings*

Questions with respect to the current application of control markings authorized by earlier directives on the dissemination and control of intelligence and utilized on documents issued prior to the date of this directive should be referred to the originating agency. These markings are: WARNING NOTICE-SENSITIVE SOURCES AND METHODS INVOLVED, CONTROLLED DISSEM, NSC PARTICIPATING AGENCIES ONLY, INTEL COMPONENTS ONLY, LIMITED, CONTINUED CONTROL, NO DISSEM ABROAD, BACKGROUND USE ONLY and NO FOREIGN DISSEM.

George Bush  
Director of Central Intelligence

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/7

(Attachment)

DCI POLICY ON RELEASE OF  
FOREIGN INTELLIGENCE TO CONTRACTORS<sup>1</sup>

1. In order that the Intelligence Community agencies may more effectively discharge their responsibilities and without intent to limit such broader authority or responsibility as any may now have under law, NSC Directive or special agreements among them, selected intelligence<sup>2</sup> may be made available by recipient officials of the Intelligence Community agencies or their designated subordinates to certain contractors without referral to the originating agency, provided that:

a. Release<sup>3</sup> shall be limited to private individuals (including consultants) or organizations certified by the Senior Intelligence Office of the sponsoring Intelligence Community agency as being under contract to the United States Government for the purpose of performing classified services

<sup>1</sup> "General policy is set forth in DCID No. 1/7, 'Control of Dissemination of Foreign Intelligence,' effective 18 May 1976. In accordance with paragraph 5a(3) of DCID 1/7, the Intelligence Community agencies agree that government-owned, contractor-operated laboratories performing classified services in support of the intelligence mission of the Energy Research and Development Administration, which are designated authorized channels by the ERDA Senior Intelligence Officer, are not considered contractors for the purposes of this policy statement."

<sup>2</sup> This directive deals solely with foreign intelligence, which for purposes of this directive, is defined as information reports and intelligence produced and disseminated by CIA, INR/State, DIA, NSA, ACSI/Army, Naval Intelligence Command, ACSI/Air Force, ERDA and the military commands. This specifically excludes Foreign Service reporting and Sensitive Compartmented Information\* (SCI). Permission to release Foreign Service reporting must be obtained from the Department of State, and permission to release SCI must be obtained from its originator. SCI is covered specifically by paragraph 3 of this directive, in that it bears one or more codewords or special instructions which dictate handling in special dissemination channels.

\*The term "Sensitive Compartmented Information" as used in this directive is intended to include all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include RESTRICTED DATA as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.

<sup>3</sup> Release is the visual, oral or physical disclosure of classified intelligence material.

in support of the mission of a member agency,<sup>4</sup> his department or service,  
as ~~Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4~~

b. The responsibility for ensuring that releases to contractors are made pursuant to this policy statement shall rest with the Senior Intelligence Officer of the sponsoring member agency (i.e., the chief of the intelligence component seeking release on his own behalf or on behalf of a component within his department or service) or his designee.<sup>5</sup>

c. The agency releasing the intelligence material shall maintain a record of the material released and shall upon request report such releases to the originating agency.

d. Intelligence material released to a contractor does not become the property of the contractor and can be withdrawn from him at any time. Upon completion of the contract, the releasing agency shall assure that all intelligence materials released under authority of this agreement and all other materials of any kind incorporating data from such intelligence materials are returned to the releasing agency for final disposition.

e. Contractors receiving intelligence material will not release the material (1) to any activity or individual of the contractor's organization not directly engaged in providing services under the contract, nor (2) to another contractor (including a subcontractor), government agency, private individual or organization without the consent of the releasing agency (which shall verify that the second contractor has a need-to-know and meets security requirements).

f. Contractors will ensure that intelligence material will not be released to foreign nationals whether or not they are also consultants, US contractors or employees of contractors, and regardless of the level of their security clearance, except with the specific permission of the originating agency.

g. Contractors shall be required to maintain such records as will permit them to furnish, on demand, the names of individuals who have had access to intelligence materials in their custody.

h. Contractors may not reproduce any material released without the express permission of the agency having contractual responsibilities. All requirements for control and accountability for original documents as indicated above shall apply equally to copies made.

2. The following intelligence materials *shall not* be released to contractors:

National Intelligence Estimates (NIEs), Special National Intelligence Estimates (SNIEs), National Intelligence Analytical Memoranda and Inter-agency Intelligence Memoranda are not releasable and hence shall bear the

<sup>4</sup> Non-Intelligence Community government components under contract to fulfill an intelligence support role, may be treated as members of the Intelligence Community rather than as contractors. When so treated, it shall be solely for the specific purposes agreed upon, and shall in no case include authority to disseminate further intelligence material made available to them.

<sup>5</sup> Releasing agencies are required to delete: a) the CIA seal, b) the phrase "Directorate of Operations," c) the place acquired, d) the field number, and e) the source description from all CIA Directorate of Operations reports passed to contractors, unless prior approval to release such information is obtained from CIA.

↑  
should state that  
procedures must  
be included in  
contracting

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4

NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS stamp. However, information contained therein may be made available, without identification as national intelligence, over the byline of the Senior Intelligence Officer of the Intelligence Community agency authorizing its release.

3. The following intelligence materials *shall not* be released to contractors unless special permission has been obtained from the originator:

Materials which by reason of sensitivity of content bear special markings, such as NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS or CAUTION—PROPRIETARY INFORMATION INVOLVED contained in DCID 1/7 (effective 18 May 1976) or which are marked for handling in special dissemination channels.

4. Questions concerning the implementation of this policy and these procedures shall be referred for appropriate action to the Security Committee.

Approved For Release 2006/04/19 : CIA-RDP86-00674R000300080023-4