

Administrative - Internal Use Only DD/A Registry
File DTM-2-1

17 DEC 1976

MEMORANDUM FOR: Inspector General

FROM : Robert W. Gambino
Director of Security

VIA : Deputy Director for Administration ^{W/S/du} 21 DEC 1976

SUBJECT : Office of Security Survey Report (Draft)

REFERENCES : (a) Memorandum to the Director of Security
from IG dated 23 November 1976, same
subject

(b) Memorandum to the Director of Security
from IG dated 13 December 1976,
subject: Revisions to the Office
of Security Survey Report

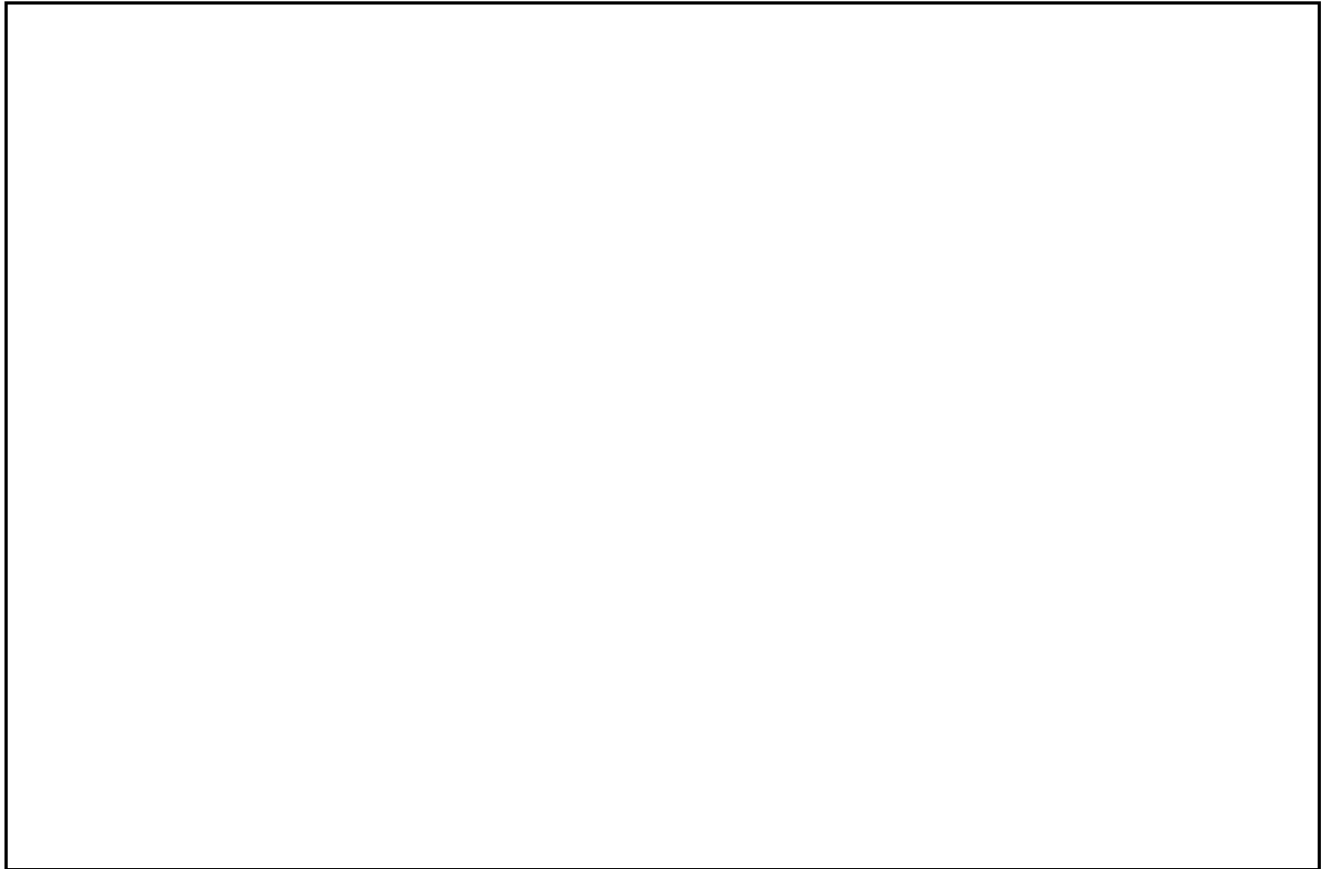
1. Pursuant to your request this Office has reviewed the draft report and offers the following comments for your consideration.

2. We must emphasize that this Office never recommended any kind of crash project to purge our records. We did offer alternatives to fulfill this commitment (Attachment 2, Annex A), one of which projected a two-year completion date contingent upon the addition of thirteen new slots to accomplish this task. Recognizing the improbability of acquiring any additional slots and for other reasons set forth in Attachment 2 of Annex A, we specifically suggested a more moderate, less disruptive program that could be accomplished within the existing ceiling. Any significant diversion of manpower to accomplish the recommended two-year crash program would evoke an intolerable disruption of our regular activities.

OS 6 5213

Administrative - Internal Use Only

25X1C



4. The draft report suggests (page 4, paragraph b(1)) that the practice of furnishing information on named Americans who are not the primary subject of investigation is of questionable propriety and recommends (page 7, paragraph 9) that this practice be terminated. This Office believes that the legal judgment of the Office of General Counsel (Attachment 2, Annex B) fully supports Office of Security participation in the National Agency Check program as it is presently constituted. We do not believe that there are any grounds for compelling the Office of Security to take the lead in dismantling a valuable investigative function that has served all U.S. Government investigative agencies for many years.

5. Annex F, page F-5 paragraph 7 notes that consideration was being given to providing [redacted] with protective service. Please be advised that since the preparation of the draft report these services have been afforded the Deputy Director of Central Intelligence/Intelligence Community.

STAT

6. Overall, we find the draft report to be an objective and sincere document. It is especially heartening to note the observation that Office of Security personnel are acutely aware of the need to conduct all their activities in a completely legal and proper manner. We are thoroughly dedicated to this proposition.

[redacted]

25X1A

Robert W. Gambino

Distribution:

Original & 1 - Addressee
1 - DD/A

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

DRAFT

OFFICE OF THE INSPECTOR GENERAL
SURVEY OF THE OFFICE OF SECURITY
MARCH - AUGUST 1976

STAT

INSPECTOR GENERAL
763435

23 NOV
1976

MEMORANDUM FOR: Director of Security
FROM : John H. Waller
Inspector General
SUBJECT : Office of Security Survey Report

Enclosed is a draft of our Office of Security Survey Report. I would appreciate it if you would review this draft and return it to me by 15 December together with any comments you may have. It would be appreciated if you state where you disagree with any of the conclusions or recommendations and the reasons for any such disagreement, in order that I may consider them and report to the DDCI such differences as remain.

[Redacted Signature Box]

25X1A

John H. Waller

Attachment: a/s

cc: General Counsel

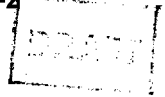
25X1

This document contains
Administrative
information for Internal Use Only
when enclosure is detached.

SECRET

US 8500

[Redacted Box]



OFFICE OF THE INSPECTOR GENERAL
SURVEY OF THE OFFICE OF SECURITY
MARCH - AUGUST 1976

25X1

S E C R E T



OFFICE OF SECURITY SURVEY

MARCH - AUGUST 1976

Background:

1. On 24 March, a four-man team of inspectors began a survey of the Office of Security (OS). By design, the survey was limited in scope. Its major thrust was to address the legality and propriety of OS activities, as distinct from a management overview of the entire Office. The last IG Survey of OS was completed in July 1973.

2. In carrying out its task, the Survey Team relied heavily on interviews at all levels within OS and a review of Agency and OS directives and OGC opinions. Considerable time was spent reviewing OS files which, in themselves, provided insights into the character and operating style of the Office.

3. Throughout the entire survey OS management was kept fully apprised of our general findings and possible problem areas. Because we were convinced that the survey report should contain no surprises for the D/OS, we undertook to resolve problems as they surfaced, rather than to await the final report. To some extent this approach has been successful. Consequently, some sections of this report will

S E C R E T

identify problems which already have been or are well on the way to being resolved by OS.

Conclusions:

4. During the course of the survey, the Survey Team was impressed by the acute awareness by OS personnel, both at Headquarters and in the field, of the need to conduct all OS activities in a thoroughly legal and proper manner. Undoubtedly, this sensitivity reflects the strong leadership of D/OS who, by his actions, has sought to insure that all OS personnel are given clear guidelines and directives that identify the policies and parameters governing OS activities. Management has gone one step further, as they have encouraged all employees to seek clarification and justification of any activity that, in their judgment, is not covered by existing Office directives or Agency regulations.

5. We found that the new operational restrictions governing OS activities have made implementation of OS mission and function more difficult. Nevertheless, we have found no evidence (except for the Polygraph Program) to suggest that these restrictions have significantly affected OS's effectiveness. In the case of the Polygraph Program, the requirement to report possible violations of law to the Department of

S E C R E T

S E C R E T

Justice reduces the atmosphere of confidentiality desirable for effective polygraph examinations. This finding pertains not only to the conduct of field investigations, but also to the handling of support functions both at Headquarters and in the field.

6. We found that, for the most part, OS is carrying out its responsibilities in a legal and proper manner. There were, however, certain OS activities that we believe to be either illegal, improper, or (if not clearly illegal or improper) to be questionable. These are briefly described below and discussed in greater detail in the Annexes, as indicated:

a. Illegal Activities:

(1) OS has considerable information on Americans in its security investigation files, collected over the past two decades; information which is now illegal to retain under the provisions of the Privacy Act of 1974 and Executive Order 11905. It would be a substantial undertaking and would take considerable time for OS to purge its files of such information. However, OS has a plan for accomplishing this in an orderly manner within a two-year period (Annex A).

25X1A

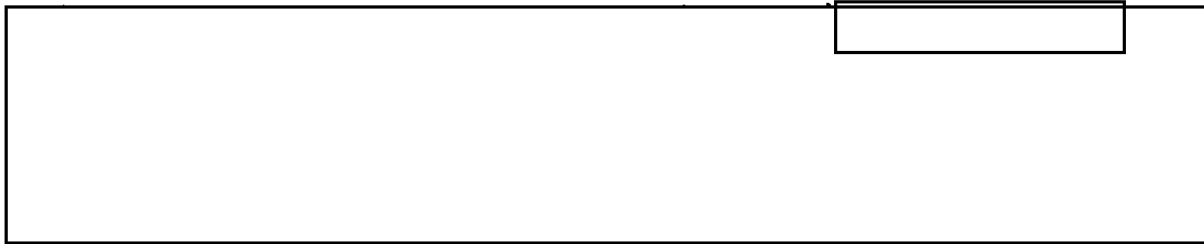
S E C R E T

S E C R E T

25X1A



(3) The authority of Agency personnel to carry firearms in the United States is limited by statute to the protection of confidential documents and materials. To provide armed protection to the DCI and DDCI, OS officers use the stratagem of having those officials carry classified documents on their person in order to technically comply with the law. As this is an area where the Agency's legal authorities is in question, OGC is actively pursuing broader legislation to clearly permit the arming of Agency officers for the purpose of protecting senior officials and Agency installations (Annex F).



25X1A

25X1A

b. Improper Activities:

(1) OS has a long-standing practice of furnishing

S E C R E T

S E C R E T

information on named Americans who are not the primary and proper subject of an OS investigation to some 50 other government agencies. While OGC has ruled this practice to be legal and OS believes it is an important and integral part of their exchange of security information with other agencies, we judge this practice to be of questionable propriety on the grounds that it permits the unnecessary exchange of unverified and unrecorded derogatory information on Americans without their knowledge or permission. (Annex B).

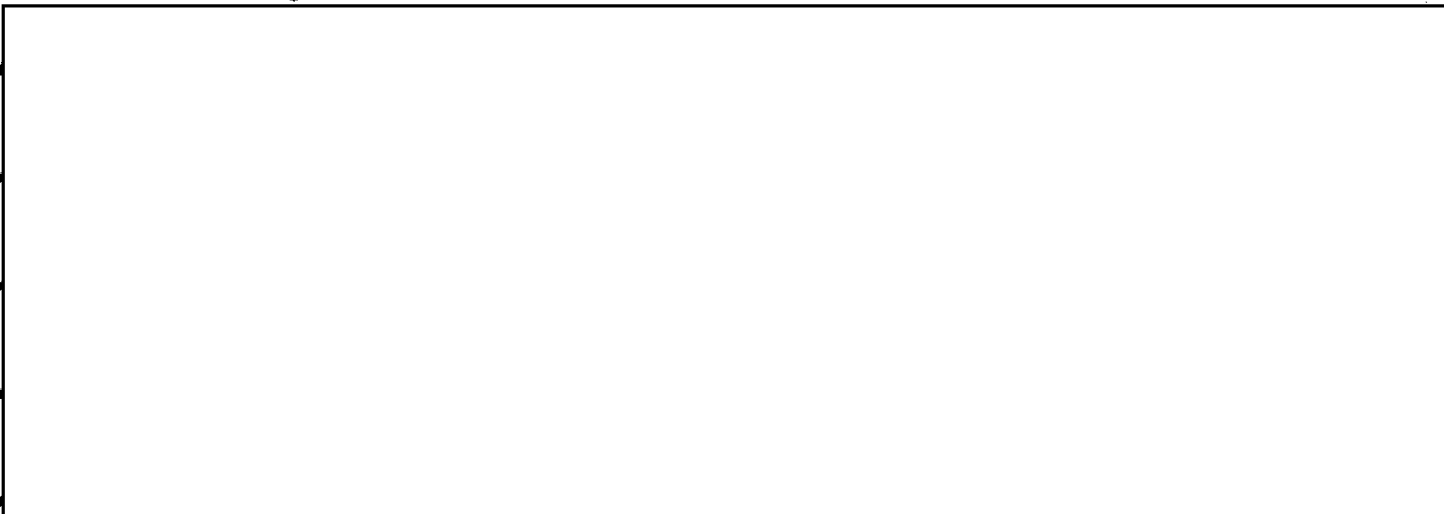


25X10

S E C R E T

S E C R E T

25X1C



c. Other Activities Which Raised Questions:

(1) OS had been using an elementary school teacher as a contract security investigator. When we questioned the merits of this relationship in comparison with the potential for unfavorable publicity, OS terminated the contract (Annex D).

(2) We found that OS personnel had questions concerning the legality or propriety of certain aspects of the polygraph program. At our instigation, OS and OGC have reviewed these issues and have resolved questions of legality or propriety. As a result, OS will develop clearer guidelines on polygraph practices (Annex C).

7. Finally, we were impressed by the openness and the spirit of cooperation shown by OS in discussing their reservations about certain of their activities and their eagerness, particularly in light of the

S E C R E T

S E C R E T

recent external investigations, to jointly seek resolution of questionable areas of activity.

Recommendations:

8. Concerning questions of illegally-held information on Americans described in Annex A, we recommend that:

a. The Attorney General and the Senate Select Committee on Intelligence be advised that, following the lifting of the Senate Moratorium and other restrictions on destruction of illegally held information on Americans, it will take considerable time to purge this information from OS files. (This topic has already been taken up with the IOB Staff (Attachment 4 to Annex A)).

b. The Office of Security institute its two-year program to identify and purge all illegally held information on Americans from its files so that OS security file holdings comport with the spirit and the intent of the Privacy Act and Executive Order 11905, when the restrictions on file destruction are lifted.

c. The Director of Security issue written guidelines specifying the type of information that may be placed in OS files and specifying the proper criterion for its indexing.

9. With respect to the question of access to OS information by other agencies described in Annex B, we recommend that the practice

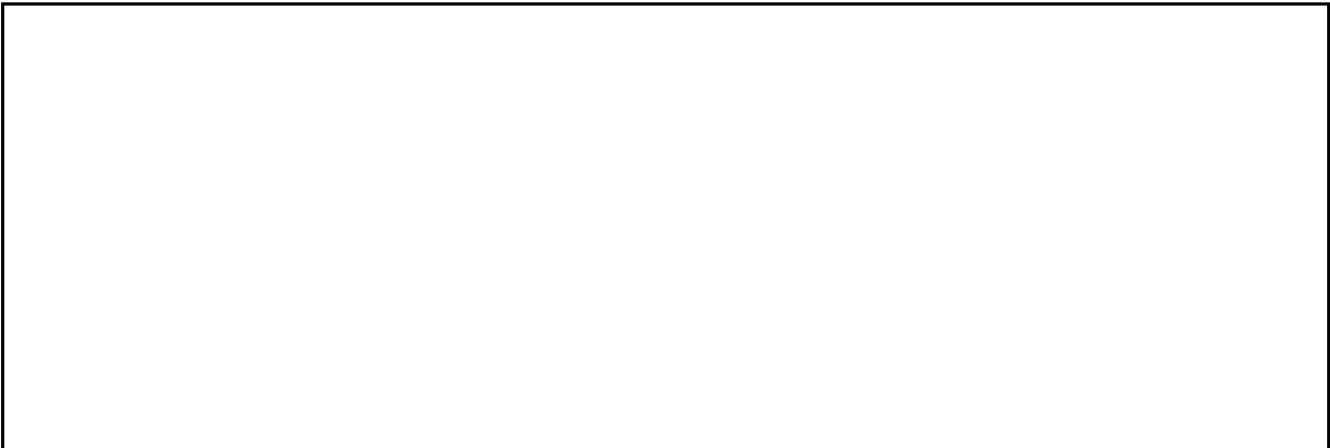
S E C R E T

S E C R E T

of providing information to other government agencies on named American citizens who are not the primary and proper subjects of OS investigations be terminated..

10. On the questions raised about the Polygraph Program described in Annex C, we recommend that the Director of Security issue updated guidance on the conduct of OS's polygraph program, incorporating the legal opinions and management policy contained in Attachment 2 to Annex C.

25X1A



12. Concerning the firearms issue described in Annex F, we recommend that explicit authority be sought through appropriate legislation for CIA to provide armed protection to the DCI, the DDCI, and such other senior officials as the DCI might name, and that legislation also provide for the specific use of armed guards to protect CIA installations in the United States.

S E C R E T

25X1

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

S E C R E T

ANNEX A

ILLEGALLY-HELD INFORMATION ON AMERICANS

Background:

1. Over the years, OS has accumulated a vast array of personal data on American citizens as a result of its security investigations of applicants, employees, contractors and their employees, and other persons with similar relationships with the Agency; as well as on persons other than the primary subject of OS investigations, intelligence sources, and corporations. In order to manage this information, OS established automated and manual indexes and dossiers for use in the initial screening of candidates for employment; in determining the security suitability of employees, contractors, etc.; in counterintelligence research; and in supporting security checks by some 50 other accredited Federal agencies.

2. These indexes and dossiers are managed by the Security Records Division (SRD) of OS. SRD indexes pertinent data identified by operating components within OS, mainly the Clearance Division, for inclusion either in the manual indexes or in the Security Automated Name Check Activity (SANCA) system. Until about 1974 there was little selectivity in the indexing process as the operative mode

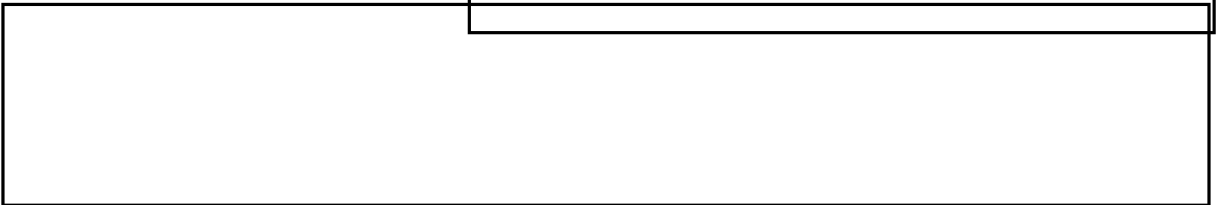
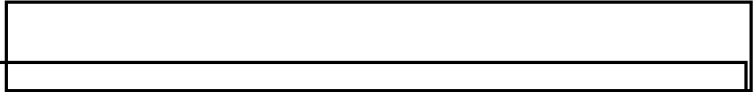
A-1

S E C R E T

S E C R E T

25X1A

encouraged over-indexing. Consequently, little information collected by OS escaped being indexed.



25X1A

3. An appreciation of how this system works and how such a massive volume of data was accumulated is described in the OS memorandum at Attachment 1. This memorandum also shows that, because of intensive indexing, OS now holds retrievable information on American citizens which the Privacy Act of 1974 describes as a "record" and thus, in certain instances, is illegal to use. Further, the limitations contained in Executive Order 11905 on collecting and storing information on "U.S. Persons" not only limit the categories of information that may be collected, but limit the range of information previously collected and currently stored.

4. As OS is well aware, the provisions of the Privacy Act of 1974 and Executive Order 11905 bear heavily on the legality and propriety of OS holdings:

a. Key provisions of the Privacy Act that apply include the following:

A-2

S E C R E T

S E C R E T

"Each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President."

"Each agency that maintains a system of records shall maintain no records describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized or a law enforcement activity."

The Privacy Act defines records as follows:

"The term record means any item, collecting or grouping of information about an individual that is maintained by an agency including but not limited to his education, financial transactions, medical history, and criminal or employment history, and that contains his name or the identifying number, symbol, or other identifying particulars assigned to the individual such as a finger or voice print or photograph." (emphasis added)

A-3

S E C R E T

S E C R E T

"The term system of records means a groups of any record under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol or other identifying particular assigned to the individual." (emphasis added)

b. Executive Order 11905 concerns itself with the same matter.

It defines collection as follows:

"Collection means any one or more of the gathering, analysis, dissemination or storage of non-publicly available information without the informed expressed consent of the subject of the information."

5. The Executive Order establishes certain restrictions on collection by foreign intelligence agencies. It restrains:

"Collection of information however acquired concerning the domestic activities of United States persons, except information concerning present or former employees, present or former contractors, or present or former employees or applicants for any such employment or contracting necessary to protect foreign intelligence or counterintelligence sources

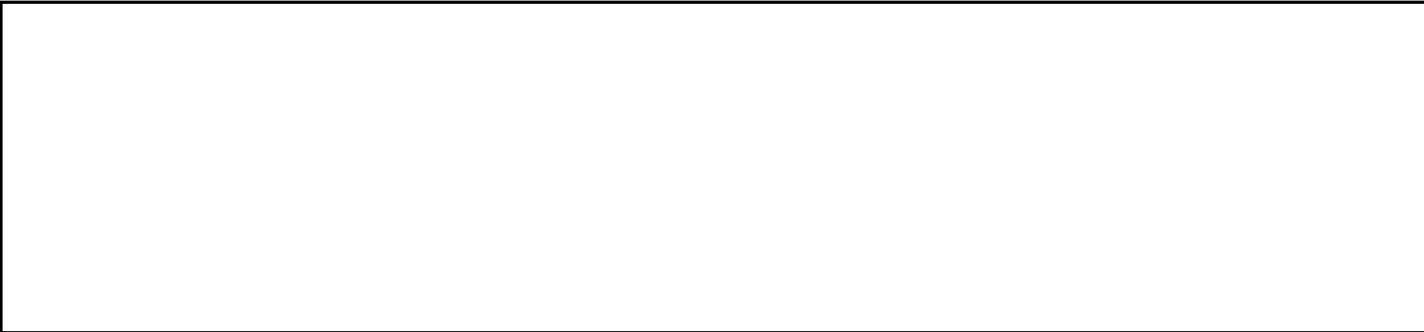
A-4

S E C R E T

S E C R E T

or methods or national security information from unauthorized disclosure; and the identity of persons in contact with the foregoing or with a non-U.S. person who is the subject of a foreign intelligence or counterintelligence inquiry." (emphasis added)

25X1A



7. OS holds a significant, but as yet unidentified, segment of records on Americans who were not dissenters; nor were they of foreign intelligence interest, nor were they relevant to the mission and function of the Agency. Although the legality of maintaining such information as separate records was not questioned prior to the passage of the Privacy Act, and the issuance of Executive Order 11905, retaining recoverable records/files on such Americans are now illegal.

8. OS had planned to purge such information from their files as a by-product of normal file use and in accordance with established National Archives and Records Service (NARS) records control schedules.

A-5

S E C R E T

S E C R E T

Under this procedure, OS estimated that it would take over ten years to complete the purging and destruction process. At our urging, OS has considered speedier solutions and estimates that they could complete a search and purge crash program in six months using 150 persons. They do not favor this approach as they feel it would seriously disrupt the normal functions of the Office. Alternatively, they estimate that the task could be completed in a two-year period using 13 people. Their views are at Attachment 2.

Conclusions:

9. OS recognizes that they are storing information on Americans that is now illegal to collect, store, and disseminate. We share their concern over the difficulties of purging illegally-held information from their files, but believe it to be in the Agency's best interests to rid itself of such holdings as soon as it is possible to do so. This should be a matter of high urgency as soon as destruction is permitted. In this connection, it should be noted that NARS records control schedules do not apply, in our view, to illegally-held information, records, and files. While we do not know with certainty what period following the lifting of the Senate moratorium and other restrictions described in

25X1A

(Attachment 3) would be allowed for the purging of illegally

A-6

S E C R E T

S E C R E T

held information from OS files, we believe that the two-year, 13 man, plan is acceptable and would accomplish this purpose in a manner consistent with protecting our security.

10. We find that OS's current input of information on Americans in its files and the indexing of this information is in accordance with the Privacy Act, Executive Order 11905, and under the close supervision of the Chiefs of the Clearance Division and the Security Records Division. However, OS's guidelines for the indexing of this information is verbal and not written.

11. Without suggesting that field investigators refrain from collecting authorized information needed to assess the security suitability of an applicant or others of similar interest to the Agency, we believe that OS should collect only such data as is relevant to the primary subject of the investigation and that this data should be kept only in the primary subject's file. No separate records should be maintained on secondary subjects unless they are of legitimate foreign intelligence or foreign counterintelligence interest.

12. As an interim measure, I have asked the DDA to issue an Agency regulation enjoining employees from using illegally held information (attachment 4).

A-7

S E C R E T

S E C R E T

Recommendations:

13. We recommend that:

a. The Attorney General and the Senate Select Committee on Intelligence be advised that, following the lifting of the Senate Moratorium and other restrictions on destruction of illegally held information on Americans, it will take considerable time to purge this information from OS files. (This topic has already been taken up with the IOB Staff (Attachment 5)).

b. The Office of Security institute its two-year program to identify and purge all illegally held information on Americans from its files so that OS security file holdings comport with the spirit and the intent of the Privacy Act and Executive Order 11905, when restrictions on file destruction are lifted.

c. The Director of Security issue written guidelines specifying the type of information that may be placed in OS files and specifying the proper criterion for its indexing.

A-8

S E C R E T

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

ADMINISTRATIVE INTERNAL USE ONLY

18 June 1976

MEMORANDUM FOR: Inspector General
FROM :
Acting Director of Security
SUBJECT : OS Record Holdings

1. On 4 June, at a meeting in Mr. Gambino's office, participated in a discussion of various aspects of the Subject. At the conclusion of that meeting these gentlemen asked that a document be prepared by this Office which would represent a comprehensive statement of what Security is now doing and sees itself able to do in the near term to reduce its excess record holdings. Subsequently a kind of "White Paper" on this Subject was prepared by this Office's Security Records Division. It is attached hereto in the hopes that it satisfies the instant requirement.

2. I will be pleased to discuss any aspect of this matter that requires further elaboration.

Att.

STATINTL

ADMINISTRATIVE INTERNAL USE ONLY

I. Security Records, Systems and Holdings

1. Security Records, consisting of indexes and dossiers, are essential to the personnel security and counter-intelligence programs of the Agency. Information in these holdings is used in the initial screening of each candidate for a security approval, for research in counter-intelligence programs, and as an orderly means for keeping information on one individual in one personal subject file. Security Records are basic tools required in the protection of sources and methods, responsibilities of the Director of Central Intelligence as established by the National Security Act.

2. A personal subject security dossier and personal subject index record(s) are established the first time an individual is processed for a security approval. Any subsequent actions or information on that individual is placed in the personal subject file. If in the course of the investigation, an FBI report is obtained on a relative, a personal reference index card is created in the name of this person. This reference index card would lead to the FBI report filed in the dossier. The requirements for extensive indexing of a report on a person other than the subject of an investigation sometimes results in a personal subject dossier being created.

STATINTL

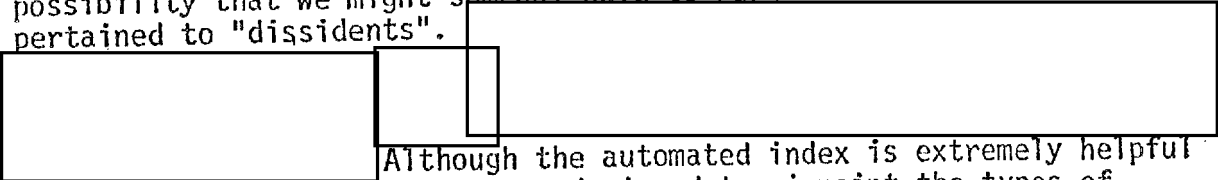


STATINTL

STATINTL



7. In developing these index and information storage systems, the primary purpose was to be able to retrieve any stored information on a person or an organization. Little consideration was given to the possibility that we might someday have to purge all information which pertained to "dissidents".



Although the automated index is extremely helpful in the purge program, it was not designed to pinpoint the types of information that we now want to purge.

STATINTL

STATINTL 8. In order to determine whether stored information pertains to a "dissident", or whether it is obsolete, one must examine the contents of the dossiers.

STATINTL

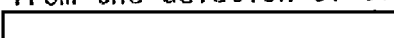
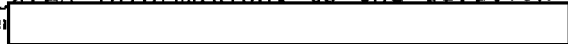
9. After deciding that a document or an entire dossier should be purged, it is necessary to locate all index records which lead to the document or dossier. Some dossiers have thousands of index records leading to them. Until the index records have been destroyed, we have not purged our holdings as intended. Failure to properly purge index records will lead to future ugly surprises and mass inefficiencies.

10. Our Security Records system is essential for proper personnel security and counter-intelligence programs. A crash program to get rid of information on "dissidents" and to get rid of obsolete material, using untrained and unqualified people who will have no future accountability, would be a disservice to the Office and the Agency.

II. Requirements for Purging

FOIAB3X

STATINTL

1. There have always been requirements for purging, ranging from the deletion of erroneous or duplicated information, to the deletion  leading to the  dossier. It is no problem, and there is very little work involved, in the destruction of such a dossier. The problem is in the location and destruction of the index records. The automated index has made it possible to accomplish purging tasks of such magnitude with no increase in SRD resources, so long as the work could be done on an "as time permits" basis.

ADMINISTRATIVE INTERNAL USE ONLY

3. We need to be concerned about our voluminous holdings of obsolete information, consisting of Security dossiers (and index records leading to them) on certain "Types of Cases" which have been inactive for specified periods of time. These were legitimate and necessary collections of information, but the information has outlived its usefulness, and is now a hindrance to efficient operations and expensive to store. Long range efficiency and economy would be served if we could apply additional resources to the task of expediting the purging of this obsolete information. In volume, it is probably ten times as great as our holdings on dissidents.

4. Our critical concern is with the question of the legality of some of our information holdings. The Privacy Act is so worded that, by some possible interpretation, it may preclude us from creating an index record and storing a document which establishes that an individual has advocated the bombing of CIA buildings. Such a person, if he just talks and takes no action, may be exercising his constitutional rights under the First Amendment.

a. The Privacy Act states that each agency which maintains records shall "maintain no record describing how an individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained, or unless pertinent to and within the scope of an authorized law enforcement activity".

b. Further, the Privacy Act states that such information can be disclosed to a law enforcement activity, "only if the head of the agency or instrumentality seeking the information or records has made a written request to the agency specifying what is desired and the reason for the request".

5. In other words, the Privacy Act is so written that it may preclude the Office of Security from maintaining information needed by the Director of Central Intelligence in order to fulfill his responsibilities (under the National Security Act) to protect sources and methods.

III. Assumptions

1. The Office of Security has proceeded on the assumption that Congress, with the Privacy Act, did not intend to relieve the DCI from the responsibility of protecting sources and methods. If he still has that responsibility, then the Office of Security has a responsibility to support him with a records system which can be used in screening candidates for security clearances, and for conducting research for counter-intelligence purposes.

2. At the same time, the Office of Security recognizes that we have considerable information holdings that are clearly inappropriate and very possibly illegal. It is our earnest desire to rid ourselves of such holdings, among which the most embarrassing are the personal subject dossiers which have been established on individuals who were dissenters, but clearly not threats to security.

3. To rid ourselves of such holdings, we have to be able to get our hands on them. We have operated on the assumption that we should place the highest priority on getting rid of the personal subject folders which hold accumulated materials on the most active "dissidents" who have never been candidates for any substantive association with the Agency.

IV. What We Have Done to Date

STATINTL

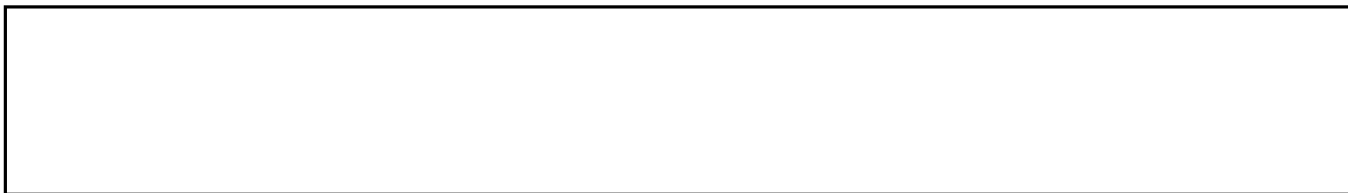
1. Proceeding under these assumptions, we have gone through all of our impersonal dossiers and selected those which are primarily concerned with dissidents. [redacted] which, in the opinions of our analysts, fell in that category. We found an additional [redacted] which, in the opinions of our analysts, contained no information of current significance from the standpoint of security or counter-intelligence; [redacted] which contained some obsolete information.

STATINTL


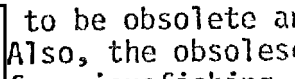
2. Our next concern was to make the best use of the impersonal files which contain information on dissidents, using information from those files as a source of "names of dissidents" on whom we may have created a personal subject file.

STATOTHR [redacted]

STATOTHR



STATINTE

4. In the meantime we had established criteria for deciding that certain information is obsolete. The same analysts who are searching for dossiers on "dissidents" have been looking to see whether the dossiers meet the criteria for obsolescent information. Analysts have identified  to be obsolete and other SRD personnel have identified  Also, the obsolescent criteria are applied to files which are candidates for microfiche. During the past three (3) months personnel of the Microfiche & Retirement Branch have identified 3151 such obsolescent files.

5. We are finding a much higher proportion of files which are obsolete than we are finding on dissidents. However, were we not approaching the task by looking for personal subject files with names extracted from the files on "dissidents" organizations, we would never achieve a thorough cleansing of our record holdings on dissidents.

6. In searching "dissident names" from the three (3) cited impersonal dossiers, we prepared cards on all unique names. We placed those cards in alphabetical sequence. We have searched our index for leads to personal subject dossiers and have reviewed all dossiers with a subject name starting with "A" through "J". We believe that we have found personal subject files on dissidents which would have remained undetected for years had we proceeded in some patently obvious fashion, such as "start with highest (or lowest) number and analyze each dossier in sequence".

7. We have prepared card decks or listings of the dossiers which our analysts consider purgable.

V. Plans

1. We plan to continue the procedures which have led to the ferreting out of personal subject dossiers which were created because of our prior interest in dissidents. This will require searching names starting with "K" through "Z" (from our "dissident names" deck) and analyzing the dossiers which bear those names.

2. We plan to obtain more definitive criteria as to the types of information holdings which are legal. We now believe that the best way to do this will be to massage some actual examples of information holdings which seem valuable from the standpoint of security, but which may be of questionable legality under the Privacy Act.

ADMINISTRATIVE INTERNAL USE ONLY

3. Once such criteria are established, we would purge all holdings which are illegal as quickly and thoroughly as can be done with suitable resources which can be found for the task.

4. After such illegal information is purged, we plan to use those suitable resources in an accelerated program to purge our holdings of useless and obsolete information.

VI. Resources needed if OS is given a deadline of 31 December 1976 to rid itself of all holdings on dissidents.

1. In order to estimate resources, we need to understand more precisely what is meant when we undertake to rid ourselves of "all holdings on dissidents". If we investigated Jane DOE as an applicant, and found that her father was an active member of the [redacted] Party, are we to remove that information concerning her father? If so, then we will have to look at each page in each Security dossier, cut out portions of pages or re-type them, and carefully trace down and remove all index records which lead to the excised information.

STATOTHR

STATINTL

2. Using round numbers, [redacted] Security dossiers. Assume that a task force would be assembled, and that there would be 100 working days remaining in calendar year 1976. [redacted] dossiers would have to be completely processed on each working day. The task force would consist of dossier analysts, clerk typists, indices clerks, file clerks and keypunch operators. A proficient analyst might be able to complete his part of the work on 100 dossiers per day, [redacted] would be required to complete the work by the deadline. Assuming that two (2) analysts could keep one clerk typist busy (excising or re-typing, and maintaining records required to control the operation), we would need 40 clerk typists. In addition, we would need 10 each of indices clerks, file clerks, and keypunch operators. Thus, to even attempt a thorough purge of all holdings on dissidents, we would need a task force of 150 people. In order to operate efficiently, these 150 people would have to be located in contiguous space in the vicinity of the shelves which hold most of our dossiers. Prior to beginning the task, these people would have to be provided clear and concise instructions. Throughout the task, close supervision and controls would have to be applied.

STATINTL

STAT

3. We believe that such a massive crash program could not be properly administered and controlled. We do not recommend it.

4. It would be more realistic to undertake to rid ourselves of impersonal dossiers which contain information about dissidents, and all of the index records leading to information in such dossiers; and rid ourselves of all personal subject dossiers which we can identify as holding information on dissidents, and all of the index records leading to such dossiers. In order to obtain most efficient use of resources, we would purge obsolete information which incidentally comes to our attention while we are attempting to identify dossiers on dissidents.

5. We will assign to the task such suitable personnel as are available, and attempt to accelerate the progress which we have made during the past year.

6. Acknowledging that we will not, with an operation of this scope, rid ourselves of all information on dissidents, we feel that we would be achieving the maximum results with resources at our command, and this is the course which we recommend.

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Next 2 Page(s) In Document Exempt

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

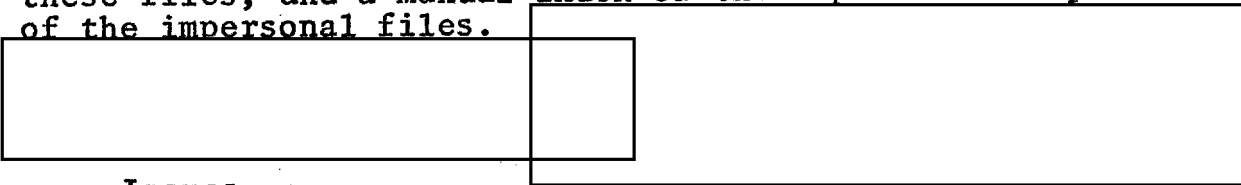
29 November 1976

SUBJECT: Purging of Security Files - Issues and Options

Security Records:

The principal record holdings of the Office of Security consist of dossiers and indices thereto which are essential to the personnel security and counterintelligence programs of the Agency. For the most part they involve file material on individuals, American and foreign, and organizations who are and/or have been of Security interest to the Agency. Security records are comprised of personal subject files, impersonal files, an automated index of individuals who are the subject of or are mentioned in these files, and a manual index of the impersonal subjects of the impersonal files.

STATINTL



Issues

STATINTL

Beginning during the 1975 investigation of CIA activities within the United States by the Rockefeller Commission, serious questions have arisen concerning the propriety of some files and records maintained by the Office of Security. These questions were first brought to a head by Recommendation (17) of that commission which read:

"All files on individuals accumulated by the Office of Security in the program relating to dissidents should be identified, and, except where necessary for a legitimate foreign intelligence activity, be destroyed at the conclusion of the current congressional investigations, or as soon thereafter as permitted by law."

25X1A



Other aspects of the Rockefeller investigation as well as the legislative inquiries that followed raised additional questions about the propriety of files maintained in our holdings on United States citizens whose affiliation with the Agency is or has been less than direct. A provision of the Privacy Act of 1974 added additional fuel to consideration of the problem in that it spoke of the maintenance of records reflecting how a citizen exercises his first Amendment rights. Executive Order 11905 established some guidelines concerning the propriety of Agency records, which also contributed food for the consideration of the problem. In addition, of considerable importance in developing an approach to the records purge issue has been our own experience in handling requests for information under the Freedom of Information Act and the Privacy Act. This experience has not only taught us a lesson concerning the embarrassing nature of some of our holdings which are releaseable under the provisions of this legislation, but has also demonstrated that a considerable amount of material in our records is clearly obsolete.

Considerations

While a review of the above issues might lead one to a sudden decision to undertake a massive purge of Security records, other considerations dictate a significant degree of caution should be exercised in approaching the problem.

Most important among these considerations is the fact that our security records are indeed essential elements in our personnel security and counterintelligence programs. A massive crash effort to purge such records would have a seriously adverse impact on these programs. While we are convinced that among these records there is a considerable amount whose propriety is questionable and whose utility is obsolete, we are equally certain that the vast majority of the records are legitimately maintained and necessary to the execution of our responsibilities.

Secondly, efforts to purge our files have been and still are encumbered by the moratorium on the destruction of Agency file materials. In the case of security files this moratorium is drastically complicated by the requirement to maintain (who knows for how long?) even questionable files, if they are related to cases in litigation.

Above all, the most substantial inhibiting factor dictating caution in any purge program is the manpower problem. The review of all security dossiers for questionable and obsolete material in itself is of great proportion. The magnitude of this job, however, is increased in geometric proportion by the need to purge simultaneously their indices. In order to maintain our file system as a going concern, one cannot be purged without the other.

Efforts to Date

Since early in 1975 when the overall problem was first recognized, the Office of Security has pursued a vigorous if modest program aimed at the identification of questionable and obsolete file material in our security records. On an average this program has encompassed the full time services of two individuals and those of one part time employee. This

which the analysts participating in the program consider to fall in the "dissident category" and/or to represent obsolete information. With the exception of the part time employee, an annuitant on contract, these results have been achieved within existing ceiling.

At the same time we have begun to establish new criteria for determining when file material becomes obsolete and purgeable. We have also taken action to prevent the initial filing of material, the propriety of which is interdicted.

Options

It is not debatable that the problem of purging security records of questionable and obsolete material requires our continued attention. The question is only one of approach.

On the one hand we can continue the direction of our efforts to date within existing resource limitations, supplemented in the future as ad hoc and temporary manpower requirement troughs occur. We would also under this option, develop an automatic purge process similar to that extant and routine prior to the Rockefeller Commission investigations. This supplemental purge process would mandate a review for questionable and obsolete material of every file "pulled" from our records by any professional in the office. This option has the obvious disadvantage that the purge effort would extend over at least ten years.

STATINTL

On the other hand we could institute a crash purge program on a task force basis. Such a force would be totally dedicated to the locating and purging of materials and index records in our file system which would qualify for purging for any reason. Such an effort would require close supervision and control. A review of the task force approach suggests that with a two year target date for completion a complement of thirteen people would be required including a project leader, six analysts, and six clerical employees. In approaching such a task in this manner we feel less than comfortable with our estimate, but more important we are concerned that the impetus of the purge syndrome may likely include babies in the bath water that is thrown away.

Conclusion

While the results of our efforts to date in identifying for disposal dissident and obsolete material in our files have been moderate, they have been significant and accomplished within resource limitations. These efforts have been successful in avoiding the pit falls of a sudden mass purge and they have not taken away from the other efforts of the office aimed at more positive goals.

We believe that our approach to the problem should continue along this approach, complemented by the periodic assignment of additional personnel, probably in small numbers and spasmodically, when other Office requirements may enjoy temporary lull periods, and further supplemented by the initiation of an automatic purge review program involving all our officers when they "pull" files for other purposes.

We do not recommend a crash program for reasons outlined in the preceding section. Not only do we feel that such a crash program would be counterproductive, but there is no way that we could undertake such a program and assign the necessary personnel resources without seriously impairing other office requirements. If it is determined that we must undertake a crash program of the magnitude described, the only way it can be done is through the assignment of additional positions to the Office of Security.

Attachment 2, Annex A, is being revised
by OS and will be forwarded separately.

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

STATINTL

RECORDS, CONTROL SCHEDULES AND THE DESTRUCTION MORATORIUM

1. CIA has statutory obligations (44 U.S.C. 33) to obtain approval of the Administrator of General Services for the retention and destruction of records. The mechanism for obtaining this approval is the submission of records control schedules to the National Archives and Records Service (NARS) for approval by the Archivist of the United States. GSA Bulletin FPMR B-62, dated 22 January 1976, requires Federal agencies to submit to NARS updated records control schedules by 31 December 1976. In a memorandum dated 20 April 1976, the DCI directed that Agency records control schedules be updated by 30 September 1976 and processed through the Directorate of Administration for approval by NARS prior to the destruction of records.

2. Senate Resolution 21, dated 21 January 1975, established the Senate Select Committee to Study Governmental Operation With Respect to Intelligence Activities. The Senate leadership requested in a letter dated 27 January 1975 that the Agency not dispose of any records or documents bearing on the subjects under investigation by the Select Committee. In a memorandum dated 28 January 1975, Mr. Colby directed that any records or documents that may have a bearing on Senate Resolution 21 not be destroyed. This was extended to include practically all Agency documents. This hold on destruction has since been referred to as "the moratorium." In a letter to the Senate leadership dated 22 June 1976, the DCI extended the moratorium on destruction of records until 10 December 1976.

3. CIA policy on destruction of records is that:

All records, including those falling under General Records Schedules, will be covered by records control schedules approved by NARS (with a copy provided to the Senate Select Committee on Intelligence) prior to their destruction.

Routine administrative records not involved under Senate Resolution 21 that are scheduled for immediate destruction will be destroyed upon receipt of NARS approval and after appropriate clearance from the Senate Select Committee.

Records involved under Senate Resolution 21 that are scheduled for immediate destruction will be destroyed after NARS approval, and appropriate clearance from the Senate Select Committee but in no case prior to 10 December 1976.

ILLEGIB

ILLEGIB

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Next 1 Page(s) In Document Exempt

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

INSPECTOR GENERAL
76-2880

MEMORANDUM FOR: Deputy Director for Administration

FROM : John H. Waller
Inspector General

SUBJECT : Suggested Regulation on Illegally Held
Information on Americans

1. This memorandum confirms our conversation of Thursday, 26 August 1976, in which I suggested that a regulation be issued to enjoin all Agency personnel from using files and records on Americans which existing law prohibits the Agency to collect, maintain or disseminate. Such a regulation would:

- a. Underscore our intention to comply with the law, and
- b. Help to mitigate the compliance problem by clarifying guidelines on what constitutes illegally held information on Americans, and on the use of such information by Agency employees.

STATINTL

2. Such files and records are now held by the Agency under a Senate Moratorium prohibiting file destruction, but in contravention to Executive Order 11905, as expressed in [redacted], and the Privacy Act of 1974. I recognize the difficulty of early and complete compliance as, in the case of the Office of Security, it is estimated that it may take some two years under optimum conditions to identify and remove illegally held information from their files. Inspectors from my Office, who have become familiar with this problem, are available to discuss details with your representative.

(signed)
John H. Waller

John H. Waller

cc: General Counsel

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

SECRET

22 July 1976

MEMORANDUM FOR THE RECORD

SUBJECT: Meeting with Messrs. Hardy and Cargal from the IOB

1. On 1320 hours, 21 July 1976 the undersigned met with Messrs. Hardy and Cargal of the IOB. These gentlemen had requested the meeting via established IG channels to discuss files and file destruction.

2. At the outset of the meeting they were both informed that I was only prepared to discuss file matters as they related to the Office of Security, because that was a subject I knew something about. Further, they were informed that the matters we were to discuss derive from an on going survey that the Inspector General was conducting of the Office of Security and that the undersigned was only one member of a four member survey team.

3. In response to a series of questions, mainly from Hardy, the following information was offered.

a. That the current problem stems from a policy followed by OS for over two decades (1950-73) which emphasized extensive indexing of documents and field investigative reports on applicants, staff employees, contractors, and people with similar employment relationships with the Agency.

b. That there were no guidelines, statutes, and or E.O.'s that prohibited such actions and that OS instituted policies, of which this was one, to insure protection of sources and methods by insuring solid security records.

c. That this indexing policy, in force for over two decades, has resulted in the collection of information on Americans, the maintainance of which is both illegal and improper under current guidelines set forth in the Privacy Act, EO 11905, and [redacted].

25X1A

SECRET

SECRET

d. That OS recognizes it has a problem and is now in the process of preparing plans to purge the holding once the existing file destruction moratorium is lifted.

e. That the problem is difficult. Its solution will require time and manpower. Files on dissidents represent only a small portion of the questionable holdings. Indeed, they have already been identified and can be purged in relatively short order. However, we still need to size the remaining problem area and in the end we may have to review all 920,000 security dossiers to excise all illegal information. After we do that we will then have to remove all records from the automated name index.

4. Mr. Hardy then suggested that as long as we removed the data from the file we would not have to worry about the index for compliance with EO 11905. I reminded Mr. Hardy that we are guided not only by EO 11905 but also the Privacy Act which as a Federal statute takes legal precedence over an Executive Order. He agreed.

5. I suggested to Hardy and Cargal that the IOB can be of help in this matter of file destruction by providing some guidelines on how much time we can reasonably have to destroy those files and records we should not be maintaining once the moratorium is lifted. I emphasized that we cannot redress ills that have accumulated for some 20 or more years overnight; that we have identified the problem but need time to institute destruction procedures and carry them through effectively.

6. To a series of other questions I assured both men that

a. OS does little or no indexing now and what is done is tightly controlled.

25X1A

c. Other files such as those maintained by DDO/CI may have some information duplicative of that in OS files, but that I reserve my judgement inasmuch as the survey team did not review such CI holdings.

7. Toward the end of the meeting both Hardy and Cargal raised the issue of dissemination of OS information. I told them that our preliminary findings indicate that security data dissemination procedures now in face by OS in its relations with 50 other government agencies may involve

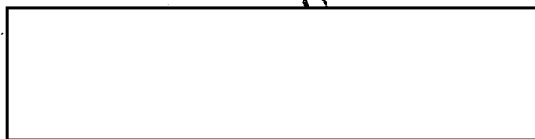
SECRET

SECRET

transfers of data on American citizens that are improper and may indeed breach the spirit and intent of the Privacy Act. I emphasized that the IOB should take no action on this matter until the survey team has a firmer base of inquiry and if our preliminary judgements are borne out, the Inspector General will initiate appropriate action. They both agreed and the meeting concluded about 1420 hours.

Comments

Hardy's and Cargal's rather precise questions led me to inquire toward the end of the meeting what information had been made available to them by the IG and the Deputy, IG. They told me that they had seen the package of material I had prepared for the Deputy IG on the general subject. They then asked for clarification on some aspects of an OS memo prepared for the survey team which I provided forthwith.



25X1A

SECRET

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

S E C R E T

ANNEX B

ACCESS BY OTHER AGENCIES TO OS SECURITY FILES

Background:

1. More than 50 agencies in the Federal Government that conduct National Agency Checks have access to investigatory information in OS files. A list of these agencies is at Attachment 1. These files contain the results of OS investigations of applicants, employees, contractors, and other persons with similar associations with the Agency - individuals (in many cases, U.S. citizens) who have specifically authorized CIA to release information about them to other government agencies. These files not only contain information about the primary subject of an OS investigation, but also contain information - sometimes derogatory - about secondary persons associated in some way with the primary subject of an OS investigation. When OS receives a request for a name check on an individual who is the primary subject of an OS file from designated representatives of one of these agencies, OS shows the representative a sanitized version of the subject's security file. This version contains only the subject's Personal History Statement and OS field investigation reports. It does not contain information from polygraph examinations, nor does it contain the basis of OS's security

B-1

S E C R E T

S E C R E T

determination if it is based on polygraph results. The representatives may not remove the sanitized file from OS, but they may extract any portion of its contents. OS keeps a record of the inquiry. No record is kept on what information is extracted.

2. This means that other agencies may extract information on secondary persons in an OS file on a primary subject (applicant, employee, contractor, etc.) without the knowledge or permission of the individual concerned. It also means that no record is kept of the fact that such information has been provided to another agency and no effort has been made by OS to ensure that such information is accurate, timely, or relevant. Further, since polygraph results are not made available to other agencies, but the final OS judgement on the security suitability of a primary subject is; false conclusions on the validity of the partial information provided may be easily drawn. As a result, it is entirely possible for another agency to set up a file on an individual, using data from OS files, without the knowledge of OS.

Conclusion:

3. We find that this uncontrolled and casual transfer to other agencies of information on individuals:

- a. that has not been formally requested by another agency,

B-2

S E C R E T

S E C R E T

b. that has not been subject to a test of its accuracy, relevancy or timeliness.

c. that has been transferred without the knowledge or permission of the individual concerned, and

d. on which OS maintains no record of its transfer stretches the bounds of propriety, if not the spirit and intent of the Privacy Act of 1974. We recognize the General Counsel's ruling (Attachment 2) that this practice is legal and within the letter of the Privacy Act.

4. We further recognize the dynamics of the security suitability milieu and certainly do hold that derogatory information on primary subjects be made available to other agencies as a service of common concern. Nonetheless, we believe that it is sufficient to inform other agencies that our investigation of the subject of their inquiry surfaced data suggesting acts of moral turpitude or other matters that may condition the subject's security suitability. Yet, we believe it unnecessary and improper to identify other persons involved in the liaison, unless these other persons represent a clear threat to the Agency and/or national security. It is entirely possible, in our opinion, to delete the names of these other persons before showing

B-3

S E C R E T

S E C R E T

OS files to other agencies, without significant damage to the National Agency Check process. Accordingly, we should avoid the inequity of needlessly providing information on Americans to other agencies without their permission.

5. Notwithstanding the General Counsel's ruling and OS's concern that restricting the availability of information to other agencies may restrict the flow of security information to OS, we believe that this practice is of questionable propriety.

Recommendation:

6. Therefore, we recommend that the practice of providing information to other government agencies on named American citizens who are not the primary and proper subjects of OS investigations be terminated.

B-4

S E C R E T

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Next 11 Page(s) In Document Exempt

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

S E C R E T

ANNEX C

OS POLYGRAPH PROGRAM

Background:

1. Past Congressional interest in the Agency's polygraph program, coupled with the strong belief on part of the Agency that the polygraph program is a critical tool in the personnel security investigation apparatus and concerns expressed by OS personnel, prompted the IG Survey Team to review the polygraph program in detail to insure the program functioned in all respects within existing statute.

2. The Polygraph Branch Chief and polygraph operators were interviewed individually covering all activities of the Branch. All manuals, instructions, regulations, directives and procedures were reviewed by the Survey Team to determine if the office was operating under proper and sufficient authority.

3. Paragraph a(6) of issued in April 1976, based on Section 4c(5) of Executive Order 11905, requires Agency employees to report any information on possible violation of the criminal provisions of the U.S. Code to the General Counsel.

25X1A

4. In May of 1976 the Attorney General's office issued an interpretation of Section 4(a)(5) of Executive Order 11905. This

C-1

S E C R E T

S E C R E T

interpretation has had a significant impact on the OS polygraph program in that possible violations of the U.S. Criminal or Civil Code detected during the course of a polygraph examination must now be reported to the Department of Justice in every instance. Heretofore, certain information acquired during the course of a polygraph examination, particularly involving applicants for employment, was held on a confidential basis solely within the Office of Security. In those cases where the polygraph examination revealed an applicant had violated the U.S. Code, he was neither admitted for employment nor was the possible violation reported outside of the Agency. Under the present guidelines, an applicant must be warned that information obtained during the polygraph examination which is in violation of the U.S. Code will be reported to appropriate authorities, i.e., the Department of Justice. Experience has shown that though an applicant may be innocent in all respects from any unlawful activities, the lack of confidentiality imposed by such a warning significantly detracts from the desired atmosphere and environment which should exist during the course of a polygraph examination.

5. As a result, the Director has recommended to the White House that Section 4(a)(5) of Executive Order 11905 be amended, citing (in part) the adverse effect that this reporting requirement has on OS's use of the polygraph for security investigations (Attachment 1).

C-2

S E C R E T

S E C R E T

6. The Executive Order 11905 with attendant DOJ interpretation raised numerous questions in the minds of the OS polygraph operators, some of which in their opinion had not been satisfactorily answered. The number and scope of unresolved questions raised by the operators were of such significance that the IG Survey Team compiled a list of 22 questions to D/OS. OS referred one third of the questions to OGC for opinion. These questions and the OS/OGC answers are at Attachment 2.

7. Finally, we note the apparent inconsistency between the requirement in Section 3(d)(x) of Executive Order 11905 that the DCI "Ensure the establishment, by the Intelligence Community, of common security standards for managing and handling foreign intelligence systems, information and products, and for granting access thereto." and the practice of requiring a polygraph examination for CIA employees and assignees and NSA civilians and not for other members of the Intelligence Community who have access to very sensitive information on sensitive intelligence sources and methods, in many cases, the same information. This anomaly has raised questions on the need for CIA's polygraph examinations and compliance with the Executive Order, and has caused embarrassing problems for certain individuals, detailed to CIA from the military services. The standards established in DCID 1/14 are minimal and permit selective use of the polygraph.

C-3

S E C R E T

S E C R E T

Conclusions:

8. We have concluded that:

a. OS's polygraph program is conducted in accord with law and regulation, but that formal OS guidance on the conduct of the CIA polygraph program should be issued. We believe that such guidance would allay the questions that have arisen within OS.

b. The anomaly of requiring CIA and NSA civilians to undergo polygraph examination and not require other individuals in the Intelligence Community having access to the same or similar sensitive information on intelligence sources and methods runs counter, in our view, to the Executive Order 11905 requirement that the DCI ensure that there are common standards for access to foreign intelligence. CIA's experience with the use of the polygraph in security investigations and in screening applicants for employment has clearly demonstrated its value. We are concerned that, if polygraph examinations are not required of all members of the Intelligence Community having access to information on sensitive intelligence sources and methods, then at some point in the future CIA's use of the polygraph may be challenged.

C-4

S E C R E T

S E C R E T

Recommendation:

9. We recommend that the Director of Security issue formal guidance on the conduct of OS's polygraph program. This guidance should incorporate the legal opinions and management policy contained in Attachment 2 to this Annex.

C-5

S E C R E T

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

CONFIDENTIAL

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

CENTRAL INTELLIGENCE AGENCY

WASHINGTON, D.C. 20505

DD/A Registry

76-3974

DD/O 76-5537/1

18 AUG 1976

Executive Registry

76-8400

INSPECTOR GENERAL

76-2805

The Honorable John O. Marsh, Jr.
Counselor to the President
The White House Office
Washington, D. C. 20500

JACK
Dear John:

This letter concerns Section 4(a)(5) of Executive Order 11905 and the adverse consequences that will ensue if the CIA and the other Intelligence Community agencies are bound to conform their practices and procedures to what I regard as the unreasonable interpretation of that section that is set forth in a memorandum dated 7 May 1976 from the Office of Legal Counsel, Department of Justice, to the White House, a copy of which memorandum is attached. I would like to ask your help in obtaining some relief from that interpretation.

Section 4(a)(5) provides that senior officials of the Intelligence Community shall:

Report to the Attorney General that information which relates to detection or prevention of possible violations of law by any person, including an employee of the senior official's department or agency.

According to the attached Department of Justice memorandum, this language must be construed to require the reporting of all possible violations of federal law within the Department's investigative or prosecutorial jurisdiction, whether criminal or civil, including possible violations of the District of Columbia Code, by any person, whether or not an employee of the CIA or other Intelligence Community agency.

To begin with, you should be aware that the reporting obligations placed on Intelligence Community agencies by Section 4(a)(5), as construed by the Department of Justice to extend to the conduct of non-Government personnel and to possible civil wrongs as well as criminal misconduct, are far more

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

CONFIDENTIAL



25XT

CONFIDENTIAL

sweeping and onerous than the statutory obligations imposed on heads of all federal agencies, including intelligence agencies, by 28 U.S.C. §535. This latter statute requires only such reports as may relate to possible violations of Title 18 (Crimes and Criminal Procedure) of the United States Code by Government officers or employees. While apparently it was intended by the adoption of Section 4(a)(5) to hold intelligence agencies to a more rigorous reporting standard than is made applicable by 28 U.S.C. §535 to federal agencies in general, I feel certain that it could not have been intended to hobble the intelligence agencies in the performance of their authorized functions. Yet that will be the result if Section 4(a)(5) must be read as having the meaning and scope attributed to it by the Department of Justice. I can best illustrate this point by reference to the CIA, but I believe the harmful and disruptive impacts would be felt throughout the Intelligence Community.

Applicants.

Applicants for CIA employment, and other persons being considered for non-employment relationships with the CIA, are screened by the Office of Security. In the case of applicants for employment, the screening includes the administration of a polygraph examination, with follow-up questions often asked in order to clarify earlier responses or reactions. A good deal of personal information, some of it unfavorable, is disclosed during these screening procedures, and as a general rule that information is received in confidence. Were it otherwise -- that, to put the matter in the present context, were a formal report to the Department of Justice required whenever the CIA received any information indicating possible violations of civil or criminal law, no matter how minor such violations -- these screening procedures would cease to be effective and the pool of applicants would be greatly reduced.

Employees.

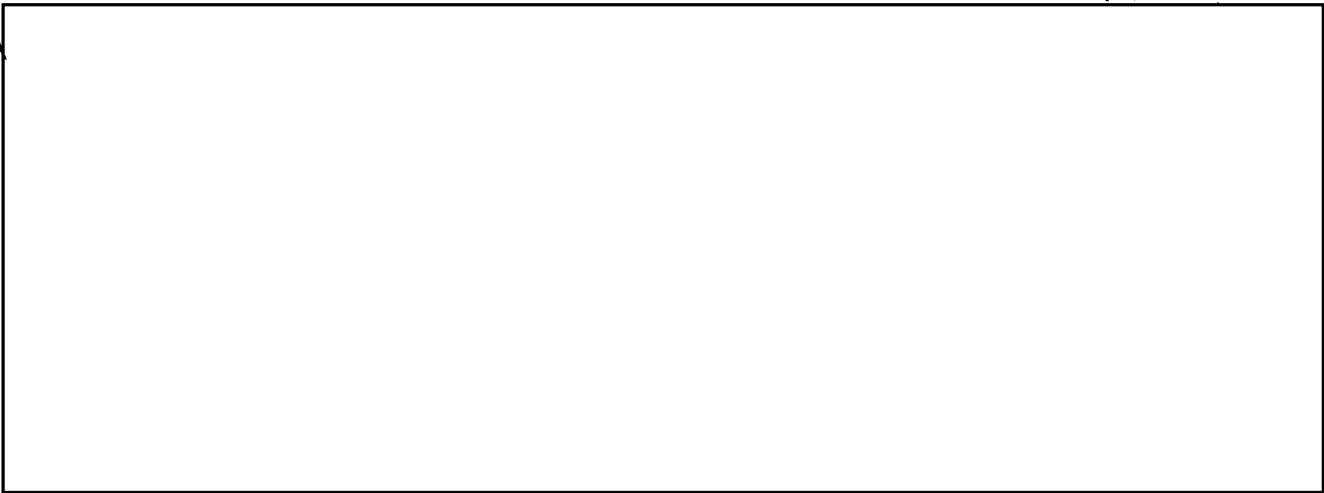
CIA employees are encouraged to be forthcoming in discussing work-related problems with their colleagues or superiors and to solicit guidance before the problems grow into serious situations. These policies would be frustrated if employees perceived that the price of frank discussion would be a report to the Department of Justice whenever there was any indication of any infraction of law, even a technical or inadvertent infraction.

U. S. Citizen Sources.

CIA contact officers often obtain valuable intelligence information on a voluntary basis from U. S. citizens, who in turn acquire that information in the course of their personal or business activities abroad. The assurances of absolute confidentiality that are customarily given to such sources would be foreclosed by the Department of Justice interpretation of Section 4(a)(5). In the absence of these assurances, much of the intelligence information now collected would never be imparted to CIA contact officers.

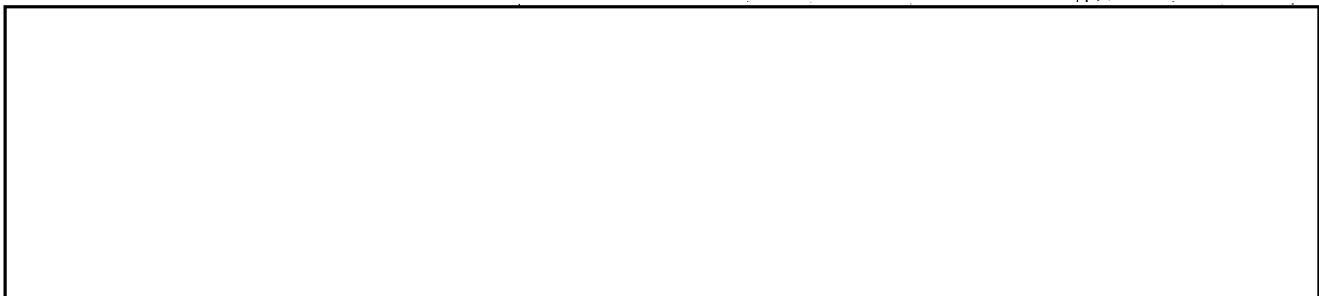


25X1A



Foreign Intelligence Services.

25X1C



In all the circumstances mentioned above, the CIA's ability to function would be seriously impaired by a strict adherence to the reporting obligations imposed by Section 4(a)(5), as construed by Justice.

As you know, the CIA and other intelligence agencies have been under intense scrutiny over the last several years. A host of procedures and restrictions have emerged from this process, restrictions which represent for the most part considered executive and legislative judgments about how the business of intelligence agencies should be conducted. In this instance, however, in consequence of the Justice Department interpretation of Section 4(a)(5), we are threatened with serious and in my view unworkable restraints that never were intended and certainly would have been rejected had they been considered, since they are fundamentally at odds with our mission.

CONFIDENTIAL

We have thus far been unsuccessful in persuading the Justice Department to alter its view about the meaning and scope of Section 4(a)(5). At the same time we have notified the IOB that we are not in compliance with the section, as construed by Justice. I am therefore appealing to your good sense and urging that you ask Justice to have a second look at its interpretation in light of this summary of our objections. If nothing can be done along this line, I believe that consideration should be given to an amendment of Section 4(a)(5). While I recognize the difficulties that stand in the way of that course, I think it would be better to face those difficulties and follow that course rather than to leave CIA and the other intelligence agencies saddled with responsibilities that were never intended and that conflict with basic intelligence functions.

Sincerely,

GB
George Bush
Director

Attachment

*Each - this matter
really needs top level
urgent attention - Thanks,
GB*

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

CONFIDENTIAL

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

INSPECTOR GENERAL
76-2425

25 JUN 1976

MEMORANDUM FOR: Inspector General
ATTENTION : Mr. [redacted]
FROM : Robert W. Gambino
Director of Security
SUBJECT : Agency Polygraph Program

25X1A

1. Reference is made to the list of twenty-two questions concerning the Agency's polygraph program which was provided to this Office by [redacted], of your Office. Transmitted herewith are our answers to fifteen of the twenty-two questions. The remaining seven questions (specifically identified in the text of the attachment) involve legal matters concerning which we are currently consulting with the Office of General Counsel. Your Office will be provided with our response to these questions following our consultation with the Office of General Counsel.

25X1A

2. In addition to the information contained in the attachment, there is a volume on the polygraph program in the Support Services Historical Series which you may find informative. This volume outlines the history of the program from its inception through 1968. The original authorization of the program is described and the subsequent approvals by various DCI's are identified. It also highlights how the program has been administered over the years and summarizes the significant developments that have occurred. There are only a limited number of copies of this history available, but one can be made available if you desire to review it.

[redacted signature box]

Robert W. Gambino

25X1A

Att :

Distribution:
Orig & 1 - Addressee

[redacted box]

25X1

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

CONFIDENTIAL

OS 6 2807

CONFIDENTIAL

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Question 1

What are the Agency requirements for the use of the polygraph?

Answer

The polygraph is used in the Agency as an aid to investigation for determining the security eligibility of persons for employment by or assignment to the Agency, security clearance by the Agency, staff-like access to sensitive Agency installations, [redacted] situations, continued access to classified information where implications of a security nature or investigative information require clarifying security interviews; and in the periodic reinvestigation of employees.

25X1A

Attached as Tab A is a list of the types of cases where a polygraph is required. Tab B is a list of the types of cases that do not require polygraph.

Question 2

What authority does the Agency have to polygraph?

Answer

The Director of Central Intelligence is responsible by law and by executive order to protect intelligence sources and methods from unauthorized disclosure. In exercising this responsibility, the DCI has authorized the Office of Security to conduct a polygraph program.

Question 3

What is the origin of this authority?

25X1

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

CONFIDENTIAL

CONFIDENTIAL

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Answer

The National Security Act of 1947 and CIA Act of 1949 and Executive Order 11905.

Question 4

Trace the source of authority from law through executive orders through Agency powers down to directives to the polygraph officer.

Answer

National Security Act of 1947 Section 102(d)(3)--
Tab C; CIA Act of 1949.

Executive Order 11905, Sections 3(d)(1)(vii) and
4(b)(8)--Tab D

25X1A



Memorandum from the DCI to the Director of Security
dated 21 February 1970--Tab G

Memorandum from Director of Security to Polygraph
Examiners--Tab H

Examiners Manual (not attached)

Also:

DOD Directive 5210.48 Section III B 3--Tab I
(For military personnel and excepted service
DOD personnel assigned to the Agency.)

Letter from the Chairman Civil Service Commission
to DDA dated 21 May 1976--Tab J (For competitive
service personnel assigned to the Agency.)

Memorandum from the Director of Security to the
DCI dated 3 February 1975, in which the DCI
approved reactivation of the reinvestigation
polygraph on 12 March 1975--Tab K

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

CONFIDENTIAL

CONFIDENTIAL

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Question 5

Are Agency regulations adequate in your opinion on the subject of polygraphing, and are these regulations available to all employees?

Answer

In our opinion the Agency regulations which grant the Office of Security authority to conduct a polygraph program are adequate in terms of giving sufficient authority to this Office. Additionally, the letter from the DCI dated 21 February 1970 is a clear mandate concerning the manner in which the polygraph is to be used within the Agency. However, in view of the date of the memorandum, this Office plans to conduct a review of its provisions and present a recommendation to the DCI that he issue an updated memorandum which will revalidate the procedures of the Agency's polygraph program.

Agency regulations concerning the polygraph are available to all employees and in conjunction with the briefing program that is carried out by the Polygraph Branch, adequate information concerning the polygraph is available to employees.

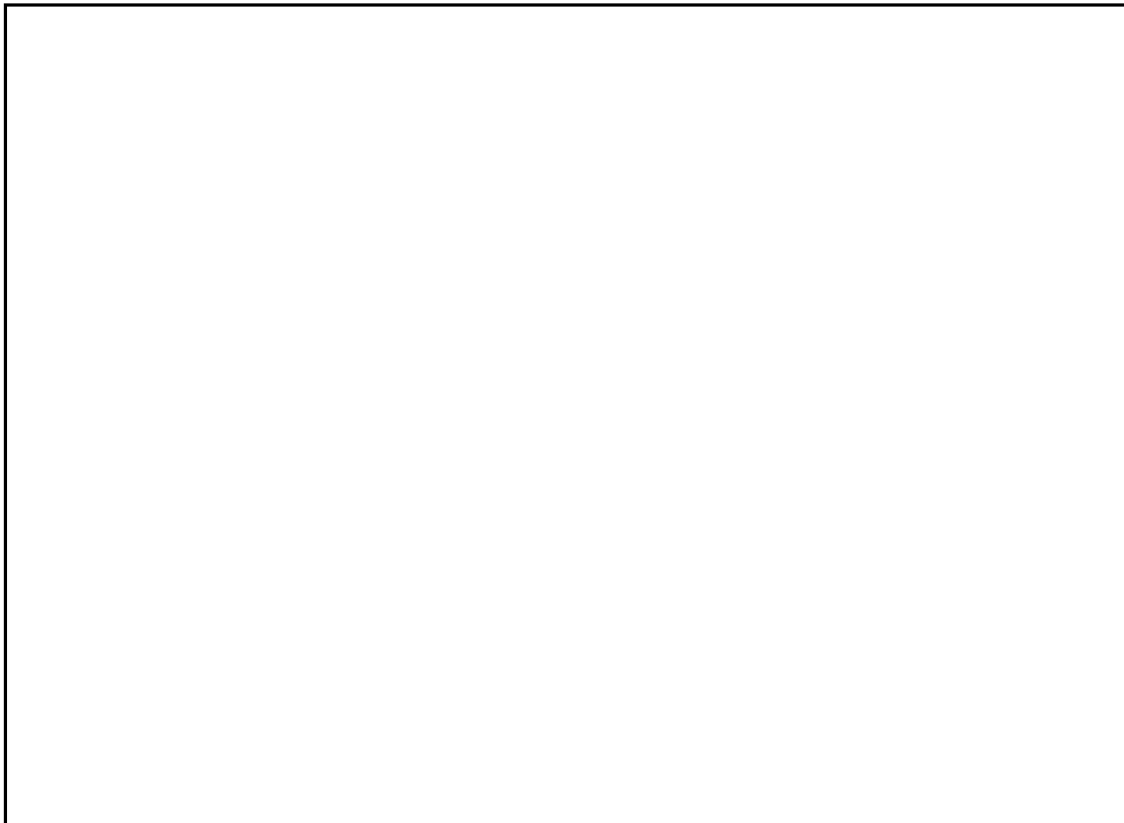
Question 6

What instructions and guidance are given to the polygraph operators as far as who is to be polygraphed, when they are polygraphed, what questions are to be asked, and under what conditions will the information be used?

Answer

Individuals to be polygraphed are those who fit into one of the categories delineated in the answer to Question 1. The examiner receives specific assignments from the Desk Supervisor in the Polygraph Branch, i.e., Staff Desk and Operational Desk.

CONFIDENTIAL



Question 7

Concerning the repolygraph program, what sanctions are imposed if a subject refuses to take the polygraph?

Answer

The reinvestigation polygraph is part of the overall security program of the Agency and as such has been approved by the DCI. Even so, there are no specific sanctions which are automatically imposed in the event an individual declines to be repolygraphed. This Office operates under a policy of making every effort to convince an employee to participate voluntarily in the program, and to date there have been no refusals. In the event an individual initially declines to undergo a repolygraph, he is referred by the examiner to the Chief of the Polygraph Branch. If the matter is not resolved

CONFIDENTIAL

at that level, the individual is referred for interviews with the DD/PSI or Chief of Operations/PSI and ultimately with the Director of Security. During these interviews, the individual is given full opportunity to articulate his reasons for declining. Following these interviews, the Director of Security decides what action will be taken. It is impossible to speculate in the abstract as to exactly what the decision would be since there are many variables which would enter into it. Of the many factors that would be considered, one of the key factors would be whether the Director of Security is convinced that the individual has some valid reason for declining the repolygraph, such as sincere religious or moral beliefs. Based on an evaluation of all factors, the Director of Security would decide whether to refer the matter to appropriate higher authority or to close the matter within the Office of Security.

Question 8

What information about the polygraph is available to applicants and Agency personnel in general?

Answer

Applicants are informed by the Office of Personnel that a polygraph examination is required as part of the processing for employment with the Agency. They are also informed that the examination will be used to verify the statements made on their Personal History Statement. Aside from this general information, applicants are given no details concerning the polygraph examination by the Office of Personnel unless they ask a specific question. At the time of the polygraph examination, the purpose and procedures of the examination are explained to the applicant and an effort is made to answer any questions the applicant may have at that time.

CONFIDENTIAL

CONFIDENTIAL

In regard to Agency personnel in general, representatives of the Polygraph Branch speak to various Agency training groups to explain the purposes and techniques of the polygraph program. In addition, when the reinvestigation polygraph program was recently reinstated, various Agency management personnel were briefed on the objectives of the program.

At the time of the actual repolygraph, every effort is made to answer any questions the subject may have concerning the polygraph.

Question 9

Should a polygraph subject confess to a criminal action, what are our legal responsibilities to report this information?

Answer

The answer to this question will be provided following consultation with the Office of General Counsel.

Question 10

What does the polygraph officer tell the person who asks if the information he reveals will be made available to anyone outside the Agency?

Answer

The answer to this question will be provided following consultation with the Office of General Counsel.

Question 11

How vulnerable is the individual examiner vis-a-vis a court suit brought by a polygraph subject: What protection can the Agency give to an examiner who is sued by a polygraph subject for invasion of privacy or denial of employment because of an admission?

CONFIDENTIAL

CONFIDENTIAL

Answer

The answer to this question will be provided following consultation with the Office of General Counsel.

Question 12

What safeguards has D/OS established to prevent unwarranted invasion of privacy during a polygraph examination?

Answer

An examiner's manual has been prepared for each polygraph examiner. The manual contains policy guidelines and explanations as to objectives that are sought in basic test coverage given to all applicants. The standard questions which are used in staff-type and reinvestigation cases have been approved by the DCI (see Tab L). Areas to be covered in specific issue polygraphs of employees must be approved by the Director of Security. Additionally, a senior supervisor/examiner electronically monitors examinations at random in order to insure that no improper conduct takes place. It should be noted that polygraph examiners are carefully selected and trained for their assignments to the Office of Security Polygraph Branch.

Question 13

What can a polygraph officer say in response to the question by an applicant: "Do I have to take this test to get a job with the Agency?" or "What happens if I don't take the test?"

Answer

Examiners have been instructed to reply that the polygraph is a necessary part of employment processing. If a subject does not take the test, then he will not be employed since he has not completed the employment processing. This is originally brought to an applicant's attention by the Office of Personnel at the time his initial processing is started. Tab M is a copy of CIA Applicant Information Sheet No. 2 which informs the applicant of the polygraph requirement.

CONFIDENTIAL

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Question 14

What is an examiner to do if a subject demands that any note or record of what he said in the interview be destroyed because he believes the test to be an invasion of privacy and says he doesn't want to be employed?

Answer

When an applicant begins his processing, he is informed that he will be polygraphed as part of the procedures and that the information in his Personal History Statement will be verified. At the time of examination, the purposes, procedures, and areas of coverage are explained and then the subject is asked to sign a polygraph agreement (copy attached at Tab N). Having voluntarily participated in the process up to this point, it would seem unlikely that a subject would terminate his interest in employment in the midst of the polygraph examination. In the event this occurred, the subject would be informed that while he was free to terminate the interview, the Agency had a right and responsibility to retain its record of what had transpired up to that point. Therefore, his request would have to be denied.

Question 15

The Civil Service Commission has recently ruled that homosexuality, per se, is not grounds to deny employment under Civil Service regulations. What is the Agency position with regard to employment of homosexuals? Is there a "per se" rule in practice in CIA against employing homosexuals? Can the polygraph officer so state to individuals?

What is the Agency position with regard to employment of homosexuals?

Answer

Homosexuals are not employed by CIA.

CONFIDENTIAL

Can the polygraph officer so state to individuals?

Answer

The role of the examiner is to obtain information which is to be used in the adjudicative process. The examiner presents himself to the applicant as an impartial fact gatherer and as not the proper person to address questions concerning the policy of the Agency. This is done so that the polygraph process is not adversely affected by the examiner becoming involved in discussions or debates concerning the Agency's policy on any particular subject. The examiner advises the applicant that questions concerning Agency policy can best be answered by other officials of the Agency and requests that he address policy questions to these officials.

Question 16

What is the Agency's obligation to report criminal information to law-enforcement authorities? To withhold such information? What happens to the legal usefulness of such information by virtue of its having been first uncovered during a CIA polygraph interview?

Answer

The answer to this question will be provided following consultation with the Office of General Counsel.

Question 17

What is the relevance of the Fifth Amendment to the CIA polygraph interview--regarding questions or admissions of criminal activity, adverse but non-criminal activity, the possibility of eliminating oneself from eligibility for CIA employment?

CONFIDENTIAL

Answer

The answer to this question will be provided following consultation with the Office of General Counsel.

Question 18

Are there Constitutional points other than the Fifth Amendment which have a bearing on the CIA polygraph interview? If so, which are those which the examiner might find more significant or which he should be prepared to explain to his subject?

Answer

The answer to this question will be provided following consultation with the Office of General Counsel.

Question 19

What are the legal parameters of the often-heard, but vague-sounding, expression "invasion of privacy," especially as it relates to CIA polygraph?

Answer

The answer to this question will be provided following consultation with the Office of General Counsel.

Question 20

During the course of a polygraph interview, an individual may give the name of another U. S. citizen (not connected with CIA) in connection with some type of derogatory activity. Is it proper to include that name in the report which is sent forward?

CONFIDENTIAL

Answer

The Office of Security is authorized to conduct a polygraph program as an aid in gathering information to be used in security evaluations. The examiner's role in this program is to gather information which is provided to those who have the responsibility for making adjudications. The operator is not in a position to make a judgment concerning the significance of a particular name or a particular item of information in terms of the overall evaluation of the case. Guidelines have been established outlining what information is required by the adjudicators and what information is the proper subject of polygraphic inquiry. Within these guidelines, the operator is obligated to report information in sufficient detail so that an informed judgment can be made by the adjudicators in any given case. Since a polygraph operator is operating within an authorized polygraph program, it is not improper for him to report the names of possibly non-CIA connected persons who may have been involved in some type of derogatory activity.

Question 21

During the course of a polygraph examination where there is an indication of wrongdoing, is the examiner only required to obtain a simple admission of a disqualifying crime, misdemeanor or felony, or is he instructed to develop a full confession? Why?

Answer

Polygraph examiners have been instructed that in the event the polygraph examination produces admissions concerning illegal or improper activity, the examiner is to continue to develop the line of questioning to obtain relevant details so that the examiner has a clear idea of what the subject is admitting. Sufficient detail will be obtained during the interview so that an accurate synopsis can be made by the examiner. This information is then forwarded through channels to the component of the Office of Security which has the responsibility to make an adjudication in the case.

CONFIDENTIAL

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Question 22

Other than employment and the repolygraph programs, under what other circumstances can the Agency use the polygraph? In what circumstances will the Agency polygraph not be used?

Answer

Aside from the polygraph requirements outlined in response to question number 1, the polygraph is also used to resolve specific allegations or issues reflecting on the continued security eligibility of Agency employees. These polygraphs are referred to as Specific Issue Polygraphs and are not conducted without the approval of the Director of Security.

The polygraph is not used by the Office of Security on official or administrative matters involving possible malfeasance, or for the sole purpose of determining violations of the criminal laws of any country.

Additionally, polygraph examinations are not given where any indications of medical or psychological problems are present, or to individuals who have not reached their 18th birthday.

CONFIDENTIAL

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Following are the types of cases where a polygraph is required:

- a. All Agency staff employees;

25X1A

- b.
- c. Independent Contractors who have staff-like access to Agency installations;
- d. Agency Consultants;
- e. Military Assignees to the Agency at Headquarters or in official Agency installations;
- f. Civilian Detailees from other Government agencies;

25X1A

- g. Career Associates who have staff-like access to the Headquarters Building or official
- h. Industrial Contractor employees who have staff-like access to Agency installations;
- i. Federal Protective Service Officers who work in all Agency buildings;
- j. General Services Administration Char Force and Maintenance personnel;
- k. Canteen Corporation Vendors working in all Agency buildings;
- l. Blind Stand Vendors in all Agency buildings;
- m. Part-time Credit Union employees;
- n. Part-time Employee Activity Association Store employees;
- o. C&P Telephone Company employees working in the Headquarters Building;
- p. Barber Shop personnel;
- q. Periodic re-investigation of staff employees.

The following cases do not require polygraph:

a. Dependent summer employees;

25X1A



c. C&P Telephone Company employees working outside of the Headquarters Building;

d. Non-Government char force and maintenance personnel (i.e., persons working for private firms)

e. Government Services Incorporated Cafeteria employees;

f. Guest speakers for various Office of Training courses;

g. One-time or short-term maintenance personnel (i.e., window washers and contract floor waxers).

CONFIDENTIAL

INSPECTOR GENERAL
76-2716

6 AUG 1976

MEMORANDUM FOR: Inspector General

ATTENTION :

[Redacted]

25X1A

FROM :

Robert W. Gambino
Director of Security

SUBJECT :

Agency Polygraph Program

1. With reference to the list of twenty-two questions concerning the Agency's polygraph program which you previously forwarded to this Office, responses to all but seven of these questions were provided to you by memorandum on 25 June 1976 (OS 62807). The remaining seven questions, which required legal opinions, had been forwarded to the Office of General Counsel for review.

2. The Office of General Counsel's responses to these seven questions (numbered 9, 10, 11, 16, 17, 18, and 19) are forwarded herewith. I have not had the opportunity to fully review the impact on the Agency's polygraph program of the legal opinions rendered in these responses, although based on my initial review I am concerned with the possible ramifications of the responses to questions 9, 16, and 18.

3. I intend to discuss my concerns with the Office of General Counsel. Following these discussions and upon completion of a thorough study of the overall effect these opinions will have on our polygraph program, I will provide you with additional comments as may be appropriate.

[Redacted Signature]

Robert W. Gambino

25X1A

Att

Distribution:

Orig & 1 - Addressee
1 - A/DDA

25X1

[Redacted]

CONFIDENTIAL

LEGAL

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Next 8 Page(s) In Document Exempt

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

S E C R E T

ANNEX D

CONFIDENTIAL CORRESPONDENTS AND PERMANENT CONFIDENTIAL INFORMANTS

Background:

1. A Confidential Correspondent (C.C.) is an experienced investigator, employed by the Agency as an independent contractor, who pro-



25X1A

25X1A

2. We reviewed the [redacted] and found that the employment of two C.C.'s appeared to be questionable. The first was an owner of a [redacted]. We asked OGC if employment of such a person by the Agency would be a violation of the Anti-Pinkerton Act. When OGC ruled that it was, OS promptly cancelled his contract. The second C.C. was an [redacted]. When we expressed our concern to OS that any publicity about this relationship (however unlikely) might have an adverse effect entirely out of proportion to the value of this relationship to the Agency, OS concurred with our observation and terminated the contract with this individual.

25X1A

25X1A

D-1

S E C R E T

25X1A

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

S E C R E T

Conclusion:

5. We believe that there may be issues of propriety involved with certain of these P.C.I. relationships. OS recognized that it may have a problem and has initiated a review with OGC. A copy of OS's plan for this review is attached. When this review is completed, OS plans to issue appropriate guidelines on the use of P.C.I.'s. We believe that this matter and the use of Confidential Correspondents is under adequate management review and that no additional action is required at this time.

D-3

S E C R E T

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Next 7 Page(s) In Document Exempt

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

S E C R E T

ANNEX F

FIREARMS -- AUTHORITY AND USE

Background:

1. Section 5(d) of the CIA Act of 1949 empowers the Agency to "Authorize couriers and guards designated by the Director to carry firearms when engaged in transportation of confidential documents and materials affecting the National Defense and Security." In an interpretation of the Act, the Office of General Counsel noted in a memorandum to the Director of Security, dated 25 February 1975, that the "restrictive terms of the CIA firearms authority contrast markedly with those of other statutes of this nature--and that--it must be assumed that the limits set out...are intended by design and not the result of inadvertence." The OGC concludes that Section 5(d) of the CIA Act, "will not support a liberal interpretation, but rather must be interpreted strictly in accordance with its terms."

25X1A

2. gives the Director of Security the authority in the Agency for issuance and control of firearms to Agency personnel within the United States. The HR states that "The carrying of firearms may be authorized in those cases where

(a) documents or materials of extreme sensitivity are being transported;

F-1

S E C R E T

S E C R E T

(b) classified documents or materials in bulk are being transported within the United States;

(c) the transportation of documents or materials affecting the National Defense involving unusual risk or security hazard due to the duration or condition of travel."

3. This strict interpretation of the law placed the Office of Security in something of a quandary for, in addition to the authorized armed escort of sensitive documents and material, the office historically has deployed armed personnel to protect the Director and Deputy Director of CIA; [REDACTED]

25X1A

[REDACTED] In the memorandum cited in paragraph 1, the OGC stated the strict interpretation of the Act would seem to preclude the use of armed escorts to protect an individual whether the individual be the DCI, the DDCI, [REDACTED] The OGC suggested a way around this problem, however, in the observation that when the "DCI or the DDCI carries confidential documents the terms of 5(d) would permit an armed escort." It is on the basis of this opinion that the OS has provided armed protection to the DCI and the DDCI. The OGC regarded [REDACTED] as being consistent with the Section 5(d) of the Act.

25X1A

25X1A

25X1A

4. With two exceptions, the use of armed personnel by the Office

F-2

S E C R E T

S E C R E T

25X1A of Security in the past year has been restricted to the protection of the DCI and the DDCI. The exceptions involved the escort by personnel of the [redacted]

25X1A Ambassador Helms. Nevertheless, the Office of Security maintains a modest capability to provide armed personnel should their services be required. At the present time a total of [redacted] permits are held in the Office of Security. Of these, 20 have been issued to

25X1

25X1 [redacted] are held by the DCI Security Staff, seven are assigned to the Security Duty Officers at Langley, and three to Security Services.

5. The firearms permits are issued by the Central Intelligence Agency. The permit carries the following statement regarding purpose and authority:

"The bearer, whose photograph appears on the reverse side is engaged in the transportation and protection of classified material on behalf of the Central Intelligence Agency, United States Government.

"Pursuant to Section 5(d), Public 110, 81st Congress, the Central Intelligence Agency has authorized him to carry firearms in the performance of his official duties."

S E C R E T

In compliance with the law, the permit is signed by the DCI and countersigned by the Director of Security. Gun permits are issued only to those who have had a course of instruction in firearms and have qualified in the use of the firearm assigned to them. The permit is valid for six months at which time the holder must requalify in order to renew the permit.

6. Tight control is maintained over all weapons in accord with

25X1A
25X1A
[redacted] Excepting those carried daily by the DCI Security Staff personnel [redacted] the weapons are stored in safes and are released only on specific authority of a senior officer. Approval to carry a gun on a specific mission, other than the protection of the DCI and DDCI, must be obtained from the Director of Security.

7. As noted earlier, the protection of the DCI and the DDCI is the only purpose for which armed men are used by the Office of Security on a regular basis. The DCI Security Staff was formed for this role in 1955 and now comprises seven men qualified to carry weapons. In carrying out its protective duties, the Security Staff assigns an armed escort to accompany the Director while he travels to and from work, while he attends official functions, and while he is making public appearances. The armed escort also accompanies the Director

F-4

S E C R E T

on official trips outside Washington [redacted]. A similar service is extended to the DDCI, Mr. Knoche. (While [redacted] is not protected by the staff at this time, consideration is being given to providing this service to him also.)

8. In providing this service, the DCI Security Staff observes the letter of the law by arranging for the Director to carry a classified document while he is being escorted. But this contrivance does not appear to conform with the intent of the law, since the purpose of the armed escort clearly is to protect the Director, not to safeguard the document in his possession. The Office of Security is not comfortable with the law as it is now written and has requested legislation which will explicitly authorize the protective service it now provides. The Office of the Legislative Counsel intends either to submit a separate amendment to the 1949 Act, providing explicit authority for armed escort of senior officials, or to cover this matter in the comprehensive revision of the 1947 and 1949 Acts now being drafted and which OLC expects to present to the next Congress.

9. CIA is authorized to assist the United States Secret Service in various ways, including the assignment of armed personnel to augment the protective force of the Service. As stated in [redacted]

"CIA may provide assistance to the U.S. Secret Service in

F-5

S E C R E T

25X1A

25X1A

25X1A

S E C R E T

the performance of its protective duties in accordance with Public Law 90-331, dated 6 June 1968, which authorizes such assistance from other Government agencies."

An agreement between the U.S. Secret Service and the CIA, signed in November 1971, states: "The Secret Service, in accordance with PL 90-331, may request CIA officers and employes to be detailed to augment the capacity of the Secret Service to perform its protective duties....the officers and employes so detailed may perform armed, technical or other protective functions." The agreement goes on to note that while detailed to the Secret Service, CIA officers and employes "will come under the direction and exclusive control of the United States Secret Service..."

10. Armed CIA personnel have been detailed to the Secret Service on two occasions only: the funeral of President Kennedy and the inauguration of President Johnson. There seems to be little possibility that the Secret Service will require their service in the future.

11. Armed Office of Security personnel have been detailed on two occasions to the Department of State to assist the Department in protective duties. There is no written agreement with the Department to cover this form of cooperation. On the first of these occasions,

F-6

S E C R E T

S E C R E T


25X1A



12. Armed OS employees were loaned to the Federal Aviation Authority several years ago for a brief period to augment armed personnel available to the FAA for the Sky Marshal Program. While the services of armed OS personnel are not likely to be requested again by the FAA, we believe that as a matter of principle, armed CIA employees should not be detailed to U.S. agencies engaged in domestic law enforcement.

13. In addition to the use of armed staff employees described above, the Office of Security hires contract personnel to protect

25X1A

 The arrangements are similar in each case. Guards are hired locally and

F-7

S E C R E T

S E C R E T

placed under contract to protect a building or installation. They are armed by the Office of Security.

14. There is no clear cut statutory authority for the Agency to perform this role. As noted earlier, the CIA statute of 1949 does not authorize the use of armed men by CIA except to escort classified documents and materials. In the past, CIA has received delegation of authority from GSA to guard CIA installations, but the authority has applied only in the District of Columbia. However, Executive Order 11905 specifically authorizes CIA to "protect the security of its installations, activities, information, and personnel."

15. [redacted] armed
civilian guards have been required [redacted]

25X1A

25X1A

25X1A

[redacted] So far there have been on un-
toward incidents, but clearly the potential for trouble is there.

Moreover, the civilian guards [redacted] do not have written guide-
lines describing the circumstances under which they may use their
weapons.

25X1A

Conclusions:

16. While there is clear authority for Agency personnel to carry (and presumably use) firearms in the United States to protect classified documents, and information, the authority to carry firearms to

F-8

S E C R E T

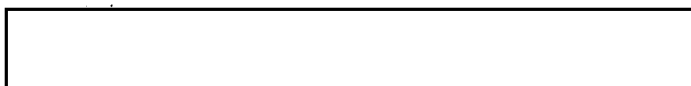
S E C R E T

protect Agency officials and facilities as such is unclear. The authority to carry firearms for these latter purposes should be clarified and appropriate guidance issued.

17. OS and OLC have this long-standing problem in hand are are seeking new legislation.

Recommendation:

18. We recommend that explicit authority be sought through appropriate legislation for CIA to provide armed protection to the DCI, the DDCI, and such other senior officials as the DCI might name, and that legislation also provide for the specific use of armed guards to protect



25X1A

F-9

S E C R E T

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Next 4 Page(s) In Document Exempt

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

SECRET

INSPECTOR GENERAL
76-3603

13 DEC 1975

MEMORANDUM FOR: Director of Security

25X1A FROM :
Acting Inspector General

SUBJECT : Revisions to the Office of Security Survey Report

1. Attached for your review are the revised versions of the summary and Annex A of the Inspector General Survey of the Office of Security. Because Mr. Blake has not seen these revisions, we have attached an extra copy for his review as well.

2. We would appreciate a response by COB 15 December.

25X1A

Attachment:
As Stated

SECRET

056 5003-2

25X1

STAT

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

S E C R E T

OFFICE OF THE INSPECTOR GENERAL
SURVEY OF THE OFFICE OF SECURITY
MARCH - AUGUST 1976

S E C R E T



25X1

OFFICE OF SECURITY SURVEY

MARCH - AUGUST 1976

Background:

1. On 24 March, a four-man team of inspectors began a survey of the Office of Security (OS). By design, the survey was limited in scope. Its major thrust was to address the legality and propriety of OS activities, as distinct from a management overview of the entire Office. The last IG Survey of OS was completed in July 1973.

2. In carrying out its task, the Survey Team relied heavily on interviews at all levels within OS and a review of Agency and OS directives and OGC opinions. Considerable time was spent reviewing OS files which, in themselves, provided insights into the character and operating style of the Office.

3. Throughout the entire survey OS management was kept fully apprised of our general findings and possible problem areas. Because we were convinced that the survey report should contain no surprises for the D/OS, we undertook to resolve problems as they surfaced, rather than to await the final report. To some extent this approach has been successful. Consequently, some sections of this report will

S E C R E T

identify problems which already have been or are well on the way to being resolved by OS.

Conclusions:

4. During the course of the survey, the Survey Team was impressed by the acute awareness by OS personnel, both at Headquarters and in the field, of the need to conduct all OS activities in a thoroughly legal and proper manner. Undoubtedly, this sensitivity reflects the strong leadership of D/OS who, by his actions, has sought to insure that all OS personnel are given clear guidelines and directives that identify the policies and parameters governing OS activities. Management has gone one step further, as they have encouraged all employees to seek clarification and justification of any activity that, in their judgment, is not covered by existing Office directives or Agency regulations.

5. We found that the new operational restrictions governing OS activities have made implementation of OS mission and function more difficult. Nevertheless, we have found no evidence (except for the Polygraph Program) to suggest that these restrictions have significantly affected OS's effectiveness. In the case of the Polygraph Program, the requirement to report possible violations of law to the Department of Justice reduces the atmosphere of confidentiality desirable for effective

S E C R E T

polygraph examinations. This finding pertains not only to the conduct of field investigations, but also to the handling of support functions both at Headquarters and in the field.

6. We found that, for the most part, OS is carrying out its responsibilities in a proper manner. There were, however, certain OS activities that are not now in compliance with existing statutes or that may be questionable, if not improper. These are briefly described below and discussed in greater detail in the Annexes, as indicated:

a. Compliance:

(1) OS has considerable information on Americans in its security investigation files, collected over the past two decades, retention of which became subject to the provisions of the Privacy Act in 1974 and Executive Order 11905 in 1976. The files are extensive, and the information that should no longer be retained is also believed to be of a very substantial volume. We recognize that it would be a substantial undertaking and take considerable time and manpower for OS to purge such information from its files. To this end, a number of options were discussed with OS -- from an accelerated, crash six-month program to a stretched-out program taking as long as ten years. Of the various alternative approaches considered, one requiring some two years to

complete seemed to offer the optimum time frame for an orderly approach to the matter, while at the same time emphasizing the Agency's commitment to bring its holdings into compliance with the new guidelines.

25X1A

(3) The authority of Agency personnel to carry firearms in the United States is limited by statute to the protection of confidential documents and materials. To provide armed protection to the DCI and DDCI, OS officers use the stratagem of having those officials carry classified documents on their person in order to technically comply with the law. As this is an area where the Agency's legal authorities is in question, OGC is actively pursuing broader legislation to clearly permit the arming of Agency officers for the purpose of protecting senior officials and Agency installations (Annex F).

25X1A



b. Questions of Propriety:

(1) OS has a long-standing practice of furnishing information on named Americans who are not the primary and proper subject of an OS investigation to some 50 other government agencies. While OGC has ruled this practice to be legal and OS believes it is an important and integral part of their exchange of security information with other agencies, we judge this practice to be of questionable propriety on the grounds that it permits the unnecessary exchange of unverified and unrecorded derogatory information on Americans without their knowledge or permission (Annex B).

(2) OS is concerned over the propriety of certain of their long-standing relationships with

25X1A

25X1A

individuals who assist OS investigators in obtaining information on subjects of OS investigations. Recognizing that there is no specific guidelines on the use of these informants, we agree with OS that there may be issues of propriety involved. OS has

25X1A

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

Approved For Release 2002/11/04 : CIA-RDP79-00498A000300100005-2

S E C R E T

(2) We found that OS personnel had questions concerning the legality or propriety of certain aspects of the polygraph program. At our instigation, OS and OGC have reviewed these issues and have resolved questions of legality or propriety. As a result, OS will develop clearer guidelines on polygraph practices (Annex C).

7. Finally, we were impressed by the openness and the spirit of cooperation shown by OS in discussing their reservations about certain of their activities and their eagerness, particularly in light of the recent external investigations, to jointly seek resolution of questionable areas of activity.

Recommendations:

8. Concerning questions of information held on Americans, described in Annex A, we recommend that:

a. The Attorney General and the Senate Select Committee on Intelligence be advised that, following the lifting of the Senate moratorium and other restrictions on destruction of information on Americans, it will take considerable time to purge such data from OS files. (This topic has already been taken up with the IOB Staff (Attachment 4 to Annex A).

b. The Office of Security institute an aggressive program of

S E C R E T

~~SECRET~~

some two years duration to identify and purge its files of all information that does not comply with the requirements of the Privacy Act and the Executive Order 11905.

c. The Director of Security issue written guidelines specifying the type of information that may be placed in OS files and specifying the proper criterion for its indexing.

9. With respect to the question of access to OS information by other agencies described in Annex B, we recommend that the practice of providing information to other government agencies on named American citizens who are not the primary and proper subjects of OS investigations be terminated.

10. On the questions raised about the Polygraph Program described in Annex C, we recommend that the Director of Security issue updated guidance on the conduct of OS's polygraph program, incorporating the legal opinions and management policy contained in Attachment 2 to Annex C.



25X1A

~~SECRET~~

S E C R E T

that consideration be given to advising the Attorneys General of those states where OS intends to continue to conduct investigations under

25X1A



12. Concerning the firearms issue described in Annex F, we recommend that explicit authority be sought through appropriate legislation for CIA to provide armed protection to the DCI, the DDCI, and such other senior officials as the DCI might name, and that legislation also provide for the specific use of armed guards to protect CIA installations in the United States.

S E C R E T

S E C R E T

ANNEX A

INFORMATION ON AMERICANS

Background:

1. Over the years, OS has accumulated a vast array of personal data on American citizens as a result of its security investigations of applicants, employees, contractors and their employees, and other persons with similar relationships with the Agency; as well as on persons other than the primary subject of OS investigations, intelligence sources, and corporations. In order to manage this information, OS established automated and manual indexes and dossiers for use in the initial screening of candidates for employment; in determining the security suitability of employees, contractors, etc.; in counterintelligence research; and in supporting security checks by some 50 other accredited Federal agencies.

2. These indexes and dossiers are managed by the Security Records Division (SRD) of OS. SRD indexes pertinent data identified by operating components within OS, mainly the Clearance Division, for inclusion either in the manual indexes or in the Security Automated Name Check Activity (SANCA) system. Until about 1974 there was little selectivity in the indexing process as the operative mode

A-1

S E C R E T

25X1A

25X1A

encouraged over-indexing. Consequently, little information collected by OS escaped being indexed. [REDACTED]

[REDACTED]
[REDACTED] that serve as reference to the impersonal subject files, i.e., files on organizations rather than people.

25X1A 3. An appreciation of how this system works and how such a massive volume of data was accumulated is described in the OS memorandum at Attachment 1. This memorandum also shows that, because of intensive indexing, OS now holds retrievable information on American citizens which it no longer can retain under the Privacy Act of 1974. Further, the limitations contained in Executive Order 11905 on collecting and storing information on "U.S. Persons" not only limit the categories of information that may be collected, but limit the range of information previously collected and currently stored.

4. OS is fully cognizant of the provisions of the Privacy Act of 1974 and Executive Order 11905 that bear heavily on the collection and maintenance of security-related information.

a. Key provisions of the Privacy Act that apply include the following:

"Each agency that maintains a system of records shall maintain in its records only such information about an

A-2

SECRET

individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President.

"Each agency that maintains a system of records shall maintain no records describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized or a law enforcement activity."

The Privacy Act defines records as follows:

"The term record means by any item, collecting or grouping of information about an individual that is maintained by an agency including but not limited to his education, financial transactions, medical history, and criminal or employment history, and that contains his name or the identifying number, symbol, or other identifying particulars assigned to the individual such as a finger or voice print or photograph. (emphasis added)

"The term system of records means a group of any record

A-3

S E C R E T

under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol or other identifying particular assigned to the individual." (emphasis added)

b. Executive Order 11905 concerns itself with the same matter.

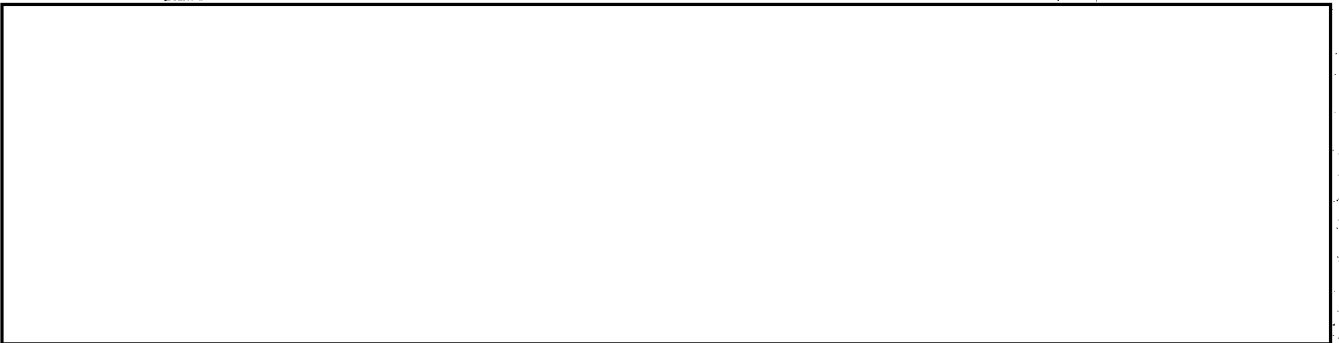
It defines collection as follows:

"Collection means any one or more of the gathering, analysis, dissemination or storage of non-publicly available information without the informed expressed consent of the subject of the information."

5. The Executive Order establishes certain restrictions on collection by foreign intelligence agencies. It restrains:

"Collection of information however acquired concerning the domestic activities of United States persons, except information concerning present or former employees, present or former contractors, or present or former employees or applicants for any such employment or contracting necessary to protect foreign intelligence or counterintelligence sources or methods or national security information from unauthorized disclosure; and the identity of persons in

contact with the foregoing or with a non-U.S. person who
is the subject of a foreign intelligence or counter-
25X1C intelligence inquiry." (emphasis added)



7. OS holds a significant, but as yet unidentified, segment of records on Americans who were not dissenters; nor were they of foreign intelligence interest, nor were they relevant to the mission and function of the Agency. Although maintenance of such information as separate records was not questioned prior to the passage of the Privacy Act, and the issuance of Executive Order 11905, compliance with the statute and the Executive Order now require such information to be purged.

8. OS had planned to purge such information from their files as a by-product of normal file use and in accordance with established National Archives and Records Service (NARS) records control schedules. Under this procedure OS estimated that ten years or more would be

A-5

S E C R E T

S E C R E T

required to complete the purging and destruction process.. We considered alternative approaches that would achieve the desired result over a shorter period of time. It was agreed that a crash program in six months, requiring an estimated 150 persons, would be disruptive and undesirable. Among the alternatives the one that seemed to us the most appropriate, in keeping with a need to address the problem with a proper priority and at the same time not be disruptive would be one with a time schedule of some two years. The number of persons to achieve this is not small, ranging from 12 to 15 persons. It was estimated that this would require either reassignment of personnel now assigned other work, or the employment of retirees; possibly a mix of the two would be indicated.

Conclusions:

9. OS recognizes that it is storing information on Americans that is not in compliance with new requirements. We share its concern over the difficulties of purging such information from the files, but believe it to be in the Agency's best interests to do so on a reasonably urgent basis once the moratorium is ended. In this connection, it should be noted that NARS records control schedules do not apply, in our view, to information, records, and files that do not comply with imperatives that

S E C R E T

SECRET

25X1A now govern Agency activities. While we do not know with certainty what period following the lifting of the Senate moratorium and other restrictions described in (Attachment 3) would be allowed for the purging of such information from OS files, we believe that such an approach would be acceptable, both in terms of orderly dispatch and security.

10. We find that OS's current input of information on Americans in its files and the indexing of this information is in accordance with the Privacy Act, Executive Order 11905, and under the close supervision of the Chiefs of the Clearance Division and the Security Records Division. However, OS's guidelines for the indexing of this information is verbal and not written.

11. Without suggesting that field investigators refrain from collecting authorized information needed to assess the security suitability of an applicant or others of similar interest to the Agency, we believe that OS should collect only such data as is relevant to the primary subject of the investigation and that this data should be kept only in the primary subject's file. No separate records should be maintained on secondary subjects unless they are of legitimate foreign intelligence or foreign counterintelligence interest.

A-7

SECRET

12. As an interim measure, I have asked the DDA to issue an Agency regulation enjoining employees from using illegally held information (Attachment 4).

Recommendations:

13. We recommend that:

a. The Attorney General and the Senate Select Committee on Intelligence be advised that, following the lifting of the Senate moratorium and other restrictions on destruction of information on Americans, it will take considerable time to purge these data from OS files. (This topic has already been taken up with the IOB Staff (Attachment 5)).

b. The Director of Security initiate a program to identify and purge all information in office files that should be removed under the Privacy Act and Executive Order 11905, with a target date of some two years for completion.

c. The Director of Security issue written guidelines specifying the type of information that may be placed in OS files and specifying the proper criterion for its indexing.