8 July 1977

MEMORANDUM FOR: John N. McMahon
Acting Deputy to the DCI for the Intelligence Community

STAT FROM: [redacted]
Chief, Security Committee

SUBJECT: PRM-29 Issues

1. Issues and options identified by the PRM-29 working groups have been combined into a consolidated report (attachment) which was sent to the co-chairmen of the PRM ad hoc committee on 6 July. The issues are to be decided as definitively as may be during a three-day ad hoc committee meeting (13-15 July), with the resultant product being circulated for formal department and agency comment. [redacted] STAT
Associate General Counsel, will represent the DCI at that meeting
STAT [redacted] will provide him back-up).

2. This memorandum is to summarize areas of apparent agreement, and state known issues with recommendations for your consideration, as they have evolved to date in the PRM-29 exercise.

a. The main thrust of PRM-29 opinion to this point would continue all of the major elements of Executive Order 11652, but impose criteria and standards where none are now provided and make existing ones more stringent. This would permit departments and agencies concerned with national security matters to continue to protect sensitive information, but will require those who are directly concerned with classification matters to give more time and attention to their actions than they now have to. The desired effect of this is to make classifications measurably more credible than they now are, and concurrently to relieve some public pressure for more openness in Government by setting up barriers to the classification of items of little or no true sensitivity.

b. Working level agreement has been reached on these specifics:

(1) Oversight for the new security classification system should be provided by an office within an existing EOP component (e.g., OMB) and headed by a Presidentially

appointed Director and Deputy. The Director is to chair an interdepartmental advisory committee similar to the present Interagency Classification Review Committee (DCI represented thereon).

(2) A range of meaningful administrative sanctions should be provided for use against those who willfully abuse the classification system (wrongful declassification as well as wrongful classification).

(3) Uniform secrecy agreements should be required from all Government employees as a condition of access to classified information.

(4) The term "national security" should continue to be defined as the sum of national defense and foreign relations matters.

(5) Specific classification criteria (i.e., descriptions of functional or subject areas requiring protection) should be provided to determine classifiability. At least one such criterion would have to be present for information to merit classification. (The level would be a separate function of the degree of damage expected from disclosure.)

(6) Paragraph classification should be mandatory, with exceptions for specific items permitted only with approval of the new oversight body.

(7) Retain that section of E.O. 11652 which requires effective protection of foreign classified information provided the U.S.

(8) Prohibitions against improper classification more specific than those in E.O. 11652 should be written into the new Order.

(9) Heads of departments and agencies should be directed to develop and use guidelines for declassifying archival material. Such use must provide for effective consultation with cooperating foreign governments on their classified information held by us (there are some differences on how this should be done).

(10) The new declassification system should:

(a) divorce period of classification from level (one effect would be to eliminate the General Declassification Schedule);

(b) limit Secret and Confidential classifiers to six-year maximum period of classification;

OUCH

(c) permit Top Secret classifiers to extend classifications past six years for specific, stated causes (comparable to present exemptions);

(d) permit classification beyond 20 years only on authority of a department head.

(11) Heads of departments and agencies should be directed to budget for and provide adequate resources to carry out provisions of the Order effectively.

(12) General declassification criteria should be specified in the Order.

(13) The mandatory review provisions of the Order should parallel those of the Freedom of Information Act (FOIA) with respect to age of material to be reviewed and to need to provide reasonably segregable portions (but much more time than the FOIA stipulates would be allowed for reviews).

c. The significant unresolved issues are:

(1) How extensive should be the appeals role of the new oversight body? The majority view is that is should be limited--i.e., to hearing appeals only on denials of declassification from requested reviews of Presidential papers 10 or more years old. This view also holds that a decision by the new body to override a departmental judgment will be suspended for 10 days to allow the department or agency head to appeal to the President's Assistant for National Security Affairs. A substantial minority wants the new body to hear and decide appeals on declassification denials under the FOIA as well. This seems adverse to the interests of the Intelligence Community--e.g., it would effectually undercut the authority of department and agency heads for final classification decisions; it would likely occupy most of the time of the new oversight body, undercutting its intended role as a useful forum for reviewing and developing classification policy.

RECOMMENDATION: That the DCI concur in the above stated majority view of the appeals role for the oversight body, and oppose any broadening of that role.

(2) What should the new Order state concerning standards and procedures for determining trustworthiness for access to classified data? This has been the most controversial issue. Defense has argued vehemently, supported by others, that the new Order should require uniform standards for investigation and adjudication of persons for access to differing levels of classified information. Their preferred option would task a component of the Executive Office of the President to develop and promulgate mandatory uniform standards (two or three) for Government-wide use in determining eligibility for access. Defense's intent is to force an end to investigative procedures, such as those prescribed in DCID 1/14, that they consider to be unnecessary and burdensome when applied to Defense personnel. The Intelligence Community has consistently opposed the Defense push in this area, not because of opposition to uniformity of standards (which is a logical goal), but because the standards Defense seeks seem quite inadequate to give minimum assurances of trustworthiness and loyalty. Community representatives in the PRM-29 forum have therefore felt compelled to argue for the status quo, under which each department and agency may amplify E.O. 10450 standards as deemed necessary. A status quo position is probably not tenable. The broad exchange of intelligence and other national security information argues for uniform standards for access to the same levels. The Community should be able to accept such, provided they were commensurate with the level of access and developed enough data to give a reasonably sound basis for confirming personal identity, and for identifying character traits indicative of trustworthiness and loyalty.

RECOMMENDATION: That if the status quo in this area becomes untenable, the DCI approve a fallback position under which the new Order would direct the attainment of uniformity in standards for determining trustworthiness for access to each of the levels of Confidential, Secret and Top Secret, through the development by the new oversight office, in consultation with the departments and agencies, of standards acceptable to all departments and agencies affected thereby.

(3) What provision should the new Order make for compartmentation? At early PRM-29 meetings, members were advised that a topic of very strong concern was the perceived need to reform practices and procedures on compartmentation. The Community is somewhat vulnerable here because it has no agreed, uniform criteria governing the establishment and review of all its compartments. We proposed criteria reflecting no more than that which we regularly expect would be done--i.e., normal safeguarding procedures must be found inadequate to protect the information; numbers of persons to be permitted access to the compartment must be kept low; and compartmentation controls must balance the need to protect against needs to use the information. These criteria found general acceptance, and were added to at the suggestion of others to require department or agency head personal approval for compartments, and to impose a three-year "sunset law" concept on existing and new compartments. The issue here is somewhat artificial, with the distinction bearing on the DCI's Community role. One option--which would require department head approval for compartments--would presumably limit the DCI's approval authority to the CIA. The other--which strikes us as unworkable--recognizes the DCI's Community role under his statutory responsibility, but would require the National Security Council to approve any other compartments (e.g., for Defense operational plans).

RECOMMENDATION: That the DCI approve criteria for compartments as stated above, and press for approving authorities to be heads of departments and agencies, or, for intelligence matters, the DCI.

(4) What provision should the new Order make with regard to classification guidelines? PRM-29 lists this as a specific topic for consideration. Two options are at issue. One, favored by departments such as State which have never developed or used classification guidance, would have the new Order make the use of classification guidelines optional. That approach is clearly contrary to the thrust of other PRM-29 evolutions, which point toward uniformity and specificity. The other would require the development and use of "general classification guidelines by departments and agencies, and encourage them to amplify such with specific guides." This would

appear to satisfy the widely shared belief that the availability and mandatory use of at least general guidance should result in better and more credible classifications. Agreement with that approach might forestall attempts to require detailed classification guides, which would be very difficult to develop for the Intelligence Community.

RECOMMENDATION: That the DCI approve support of the second option listed above.

(5) Should the new Order give special recognition to intelligence information? A proposal, offered late in the PRM-29 evolution, would have the new Order authorize "special departmental arrangements," reference statutory provisions which have some bearing on intelligence (e.g., 50 USC 403(d)(3) with regard to sources and methods, and 18 USC 798 with regard to COMINT), and proscribe automatic declassification of such intelligence. The object seems to be to focus attention on the special sensitivity of such information. The object is laudable, but the means seem likely to create problems. "Special departmental arrangements" means compartments, which are to be dealt with specifically by the new Order [see issue (3) above]. Reference to them by another name in another context would cloud the policy. Specific reference to the statutes cannot give the information involved any more status than it has now. It might invite unwelcome attention to the fact that the statutes do not provide for any specific protection for sources and methods information or COMINT. (This is unlike the case for Restricted Data, where the Atomic Energy Act provides for statutory protection wholly apart from the national security classification system.) Total exemption of such intelligence information from automatic declassification is unmanageable. We have been unsuccessful in defining where intelligence leaves off and where, for example, military operational or foreign relations plans pick up. With the above in mind, it would be helpful as an aid in bureaucratic infighting on classification to have the President give some recognition of concern for the protection of sensitive intelligence.

RECOMMENDATION: That the DCI, one, oppose having the new Order try to give intelligence a special status apart from other national security information; and, two, approve

having the new Order state the President's view that intelligence sources and methods information is particularly sensitive, and his desire that it be classified and declassified with particular care, consistent with the overall provisions of the Order.

3. A matter of concern to the Community under PRM-29 is the proposal to advance the date for automatic declassification from the present 30 years to 20 years after origin. Most involved in the PRM-29 effort apparently concluded that because the PRM asked for consideration, inter alia, of "which categories of classified material more than 20 years old could be declassified in bulk under appropriate guidelines," the issue was settled. We don't agree. While we do believe it likely that openness in Government constituencies will force serious consideration of this proposal, we believe strongly that the DCI should insure that the President and his immediate staff are aware of the resources which would be needed to deal with this change, and the consequences to national security should those resources not become available. The proposal would instantly require all classified material for the 1947-57 period to be declassified unless specifically authorized for extended protection based on individual review. That review would have to be stretched out over a number of years, and would be very expensive in terms of manpower. (The appendix to Tab F of the attachment is an assessment of the problem by Archives--it gives a rough estimate of $200 million for the review cost over a 10-year period.) That level of resources would be competing with ongoing requirements in the developing budget. If it survived, it is by no means certain that the Congress would appropriate it. (Witness what happened on resources used to handle FOIA requests.) If the resources needed for the review fell measurably short, some records within the 10-year period could not be screened, but there would be no proper authority under the Order to continue to withhold them from the public. The potential impact on sources and methods, and on foreign cooperation, could well be disastrous. We urge this be brought to the DCI's personal attention.

STAT

Attachment
As stated

TABLE OF CONTENTS

Approved For Release 2005/06/09 : CIA-RDP82M00591R000500030014-0

ISSUE: THE EXAMINATION OF THE ROLE AND EFFECTIVENESS OF THE INTERAGENCY CLASSIFICATION REVIEW COMMITTEE

DISCUSSION:

The Interagency Classification Review Committee (ICRC) was established pursuant to Executive Order 11652 and its implementing National Security Council directive. The Committee was established to assist the NSC in monitoring the implementation of the Order and was specifically charged with: (a) overseeing Departmental actions to ensure compliance with the Order and implementing directives, (b) receiving and acting on complaints or suggestions from within or without the government regarding the administration of the Order, including appeals from denials of declassification requests, and (c) developing means to prevent overclassification, ensure prompt declassification and access to declassified material, and eliminate unauthorized disclosures.

Committee membership includes representatives of the Departments of State Defense and Justice, the Archivist of the United States, the Central Intelligence Agency, the Energy Research and Development Administration and the National Security Council staff. Dr. James B. Rhoads, Archivist of the United States, was appointed by the President as Acting Chairman in April 1973. The ICRC is authorized a permanent staff of eight personnel including the Executive Director. The staff draws its support, including budgetary funding ($173,600 for FY 77), from the General Services Administration through the National Archives and Records Service.

In meeting its monitorship responsibilities, the ICRC has relied primarily on a system of quarterly oversight reports from all Departments granted original classification authority and on a system of detailed on-site program reviews of Departmental implementation. ICRC program reviews entail in-depth analysis of all facets of classification, declassification and safeguarding procedures within Departments.

Significant progress has been achieved in restoring a balance between public access to information regarding the affairs of government and protection of official information in the interest of national security. While much of the credit for this success must be given to the progressive actions taken by Departments, recognition must also be given to the fact that many of the actions were in response to ICRC oversight and reporting requirements. Examples of progress include: (a) classification authority reduction of over 76%, (b) a 65 percent reduction in unauthorized disclosures in CY 1976;

(c) the granting in full or in part of 86 percent of all requests for declassification review: (d) a 22 percent greater use of the Confidential category as compared with the use of the more restrictive Secret and Top Secret categories; (e) limiting exemptions from the automatic declassification provisions to less then 25 percent of the information classified in most Departments; (f) the declassification of nearly 200 million pages of official records under the NARS declassification program since 1972, and the declassification of millions of pages under separate Departmental programs; and (g) demonstrated public confidence in the executive declassification and appeal program by a 1400 percent increase in the number of requests for declassification review -- further substantiated by the fact that only 3 percent of the requests have been appealed to Departmental Review Committees and less than 0.6 percent have reached the ICRC appeal level.

Still, much remains to be done to ensure more effective implementation. The efforts of the oversight body can be enhanced by certain actions. The appointment of a Chairman of national stature would publicly demonstrate a commitment at the highest levels to the laudable goal of openness. Similarly, the effectiveness of the oversight body would be enhanced by the re-affirmation of the status of the body as an arm of the President. Prior to September 1973, the Committee staff was physically located in the Old Executive Office Building and the Executive Director was a member of the Domestic Council. In 1973, the staff was transferred both physically and administratively to the National Archives. This downgrading of the chain of authority from the White House or NSC has had a detrimental effect on the Committee and its work as well as on the effectiveness of the Executive Director in his relationship with Departments. The effectiveness of the Committee has also been impeded by a lack of sufficient staff personnel to carry out the Committee's extensive responsibilities. Until late 1975, the entire staff consisted of only three personnel, including the Executive Director. In August 1975, a senior program analyst was added and in 1976, four additional members joined the staff. It was only after the latter expansion of the staff that the detailed program reviews, which have become the core of the Committee's monitorship program, were undertaken.

In considering the role and effectiveness of the ICRC, the work group examined the following significant factors:

(a) The degree of independence of the body, or at least the appearance of independence from the perspective of the public.

(b) The location of the oversight body within the executive branch hierarchy and its apparent degree of authority.

(c) The composition of the oversight body and the ability of Committee members to make independent decisions.

(d) Whether the oversight body should continue to accept and act on appeals.

(e) Where overall monitorship responsibility should be placed.

(f) The degree to which the oversight body should be involved in suggestions or complaints regarding executive branch administration of the order.

(g) Whether the functions currently performed by the ICRC could be handled as effectively by an advisory board or a separate office.

(h) What additional functions should be assigned to the oversight body.

OPTIONS:

1. Abolish the ICRC. Establish a "Security Information Oversight Office" within an existing office (s) of the Executive Office of the President having current general oversight over internal operations of the government and a close relationship with the President, e.g., in the Office of Management and Budget. Overall responsibility for monitoring, policy direction and implementation of the Executive order shall rest with the head of the selected E.O.P. Office. The Oversight Office shall be headed by a Director and a Deputy Director appointed by the President. Administrative support for the Oversight office shall be provided by the selected E.O.P. Office. In addition, establish an "Interagency Security Information Advisory Committee" comprised of current membership on the ICRC which shall be chaired by the Director of the Oversight Office. The functions assigned to the new Oversight Office shall be the same as those currently assigned to the ICRC except that the new Oversight Office shall act only on those appeals involving the declassification of 10 or more year old material which is not subject to the provisions of the Freedom of Information Act, as amended. In each such instance, representatives of the Interagency Advisory Committee shall be requested to provide an advisory opinion on the declassification or continued classification of the material to the Director of the Oversight Office. In those instances where the Director of the Oversight Office decides, based on the advisory opinions, to declassify the information, such action shall not take effect for a period of 10 days, during which time the head of the affected Department may appeal the decision to the President through the Assistant to the President for National Security Affairs.

ADVANTAGES:

a. From the public perception would be a more independent and authoritative body than the current ICRC.

b. The course of action is more compatible with current plans for reorganization of the Executive Office of the President.

c. This option provides a means for the public to appeal declassification denials of that information which is not subject to the provisions of the FOIA, as amended; e.g., Presidential materials.

d. Eliminates the delays associated with action by Committee and will permit more rapid monitorship actions.

e. This option continues to permit the oversight body to draw upon Departmental resources and expertise.

f. Except for that information not subject to the FOIA, leaves the final executive branch decision on appeals with the Departments. Further, even in the case of the former, provides for advisory opinions by the Departments.

g. This option retains an interagency forum for the exchange of views and ideas on security information.

DISADVANTAGES:

a. The elimination of the appeals functions on all but information not subject to the FOIA may have a slight negative public impact.

b. This option does not provide as independent an appearance as would be obtained by a separate office in the Executive Office of the President.

2. Identical with Option 1 except that under this Option the Security Information Oversight Office would be charged with all functions currently assigned to the ICRC under E.O. 11652 plus responsibility for acting on those FOIA appeals of Departmental denials involving the b(1) exemption submitted to the Oversight Office voluntarily by requesters.

ADVANTAGES:

a. Presents the appearance of a more independent and authoritative body than the ICRC.

b. This course is more compatible with current plans for reorganization of the Executive Office of the President.

c. Since this Option provides for the hearing of both Mandatory Review and FOIA appeals it may be less susceptible to public criticism than Option 1.

d. This Option also eliminates delays associated with Committee action.

e. Retains an interagency forum for the exchange of views and ideas on security information.

f. Allows the Oversight body to continue to draw on Departmental resources and expertise.

DISADVANTAGES:

a. Adoption of this course will require a significant increase in the size of the Oversight staff, and consequently, in the selected Executive Office of the President, in order to handle and process the anticipated major increase in the number of FOIA appeals.

b. The course of action places the final decision on appeals with an oversight body rather than with the heads of Departments.

c. In all probability, the majority of the effort of the Oversight Office will be involved in the processing of appeals rather than on substantive policy and monitorship matters.

3. Retain overall responsibility for oversight of the Information Security Program in the National Security Council. Abolish the ICRC and hold the head of each Department responsible for monitoring the implementation of the program within his/her Department. Require Departmental reviews and inspections and annual reports on program progress to a designated NSC office.

ADVANTAGES:

a. The adoption of this option would place final authority in the head of the Department where responsibility for classification actions rests, rather than in an oversight body.

b. Implementation could be effected more rapidly since Departments would not be required to submit implementing regulations to an oversight body for approval.

c. Departmental reporting requirements would reduced to an annual basis rather than semi-annual as now required.

d. A slight cost savings would accrue due to the elimination of the current ICRC staff.

DISADVANTAGES:

a. There would probably be a negative public perception of this course of action -- it would be viewed as retrogressive.

b. This course of action would contribute to a lack of standardization in the application of information security procedures.

c. Experience shows that Departments will not allocate sufficient resources to effectively implement the Order -- rather, resources will be diverted to other programs or projects of greater immediate interest to the particular Department.

d. The appeal function now handled by the ICRC would have to be eliminated in the absence of an oversight body. Some other mechanism would be required to hear appeals regarding information contained in Presidential materials since such information is not subject to the Freedom of Information Act, as amended.

e. No independent external group will be available by Executive action to review, inspect or objectively analyze Departmental implementing actions.

f. In all likelihood, a slight increase in the NSC staff will be required.

g. This course of action eliminates the Interagency forum for dealing with mutual problems related to classified information.

h. This course of action is unlikely to contribute to greater openness or better protection of national security information.

RECOMMENDATIONS:

During the course of its deliberations the Sub-Group developed and considered a number of possible options. There was consensus among the members that the new oversight body should be placed in a major office within the Executive Office of the President in order to provide the body sufficient authority to carry out its monitorship functions. Similarly, there was agreement that the Oversight Office should be neaded by a Director and a Deputy Director appointed by the President and that an interagency advisory committee should be established. Members agreed that the Oversight Office should be charged with those functions currently assigned to the ICRC with one major exception. This exception was a divergence of views on whether the Oversight should act on all appeals above the Departmental level, including FOIA appeals involving the b(1) exemption, or whether the Oversight Office appeal authority should be

limited to only those appeals involving 10 or more year old material which is not subject to the provisions of the FOIA, as amended; e.g., Presidential materials. The Sub-Group recommends that the ad-hoc Committee consider both Options 1 and 2 in arriving at its decision on the oversight body.

ISSUE: What Kinds of Disciplinary Actions Can be Taken to Prevent the Misuse of the Security Classification System by Government Officials

DISCUSSION:

Executive Order 11652 expressly prohibits classification in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or a Department or to restrain competition or independent initiative. The Order also includes a general prohibition against classification "... to prevent for any other reason the release of information which does not require protection in the interest of national security." The sole administrative sanction prescribed by Section 13 of Executive Order 11652 is "administrative reprimand" and, it becomes operative only for "repeated abuse." There are no specific sanctions or range of sanctions for unauthorized release or disclosure of classified information. Classification and continuation of classification in violation of the Order are not explicitly subject to administrative sanction.

During the course of its deliberations, the Sub-Group examined the following significant factors related to the main issue:

(a) The sufficiency of sanctions currently provided in Executive Order 11652.

(b) The need for criminal sanctions for extreme misuses, such as use of classification to cover up criminal activities or gross mismanagement.

(c) The question of whether the new Executive order should require that each person who has access to classified information execute a secrecy agreement as a condition of being granted access.

(d) Preventative methods such as disciplinary measures, civil fines, criminal sanctions and increased use of polygraph tests.

The Sub-Group members were of the opinion that some sanctions are desirable for unauthorized disclosures, and that the problem of prosecuting those responsible for unauthorized disclosures may not necessarily result only from an unwillingness to pay the price of enforcing existing statutes. Rather, Sub-Group members agreed that existing statutes are generally not applicable to all unauthorized disclosures, such as anonymous leaks to the press.

Intelligence agencies have often refused, prior to any investigation of a leak, to declassify information determined to be essential for purposes of prosecution. It was the opinion of the Sub-Group members that this difficulty seems to be capable of resolution. They were persuaded that a refusal to undertake any criminal investigation without an advance commitment from the concerned agency to declassify this information not only may preclude the taking of adequate measures to prevent further disclosures,

but such policy very often may preclude fully informed and rational determination of whether or not it is actually appropriate to declassify such information or reveal intelligence sources and methods. The Sub-Group members were of the opinion that investigations may often be necessary for purposes unrelated to prosecution, such as to provide valuable insight into the vulnerabilities of security procedures or into methods for corrective management actions. Existing policy may often preclude consideration of factors necessary to an informed decision of whether or not to declassify.

During consideration of whether or not the new Executive order should require each person who has access to classified information to execute a secrecy agreement, the Sub-Group took cognizance of the following:

(a) The desirability and effectiveness of using secrecy agreements as a means of preventing disclosure of classified information was discussed in detail in the PRM/NSC-11 subcommittee report.

(b) In Executive Order 11905, the President required all employees of the executive branch and its contractors to execute a secrecy agreement as a condition of obtaining access to information containing sources and methods of intelligence.

(c) At present, most Departments and Agencies have executed agreements to comply with Executive Order 11905 but there is some question as to whether they are in full compliance. Exceptions are CIA and NSA which already have secrecy agreement programs applicable to all employees.

(d) Under the CIA and NSA programs an employee is required to execute a secrecy agreement as a condition of employment, and other persons execute such agreement as a condition of gaining access to classified information.

Agencies which now use secrecy agreements would not like to see the new Executive order contain any provision which would require their present employees to reexecute a secrecy agreement. Some members preferred a Government-wide uniform secrecy agreement as a condition of obtaining access to classified information. No member was opposed to secrecy agreements in principle. However, one raised questions about their utility as a preventative tool and felt that the beneficial returns from the use of secrecy agreements are probably far less than the administrative burdens and costs. He agreed that secrecy agreements may, in some instances, provide the Government with the legal vehicle of a civil injunction, but was not of the opinion that it will deter those who are predisposed to disclosure and will probably be demeaning and insulting to those who are not. The usefulness of the secrecy agreement in seeking an injunction, according to one member, is perhaps even more limited since the Government will only be able to seek this writ where it has prior knowledge of the planned disclosure, which will be the exception.

The Sub-Group as a whole agreed that requiring the military, career Civil Service entrants or present government employees to sign a secrecy agreement as a condition to employment may not be legally possible. However, the Sub-Group believes that requiring such persons to sign a secrecy agreement as a condition of obtaining access to classified information will not present any legal problems. The opinion was expressed that the President has the power to impose such a requirement upon the military as Commander-in-Chief of the Armed Forces, and upon career Civil Service entrants and present government employees under 5 U.S.C. 3301 and 3302.

The question was raised: Since a secrecy agreement is a contract, where is the necessary consideration when the secrecy agreement is based upon obtaining access to classified information? Members were of the opinion that the Government's consideration is the employee's promise to safeguard classified information and to refrain from disclosing the same, and that the employee's consideration is the ascertaining of a job that requires access to classified information, which he otherwise could not hold.

Also considered by the Sub-Group for inclusion in the Order was a provision calling for liquidated damages or a civil fine. One member objected to such a provision on the grounds that a civil fine could not be imposed through an Executive order, rather it would require legislation. And, while a liquidated damage clause probably could be included, it would be awkward to enforce because of the difficulty of placing a value on the classified information disclosed.

The Sub-Group considered the efficacy of the sanctions in Executive Order 11652 with respect to repeated abuse. The Sub-Group concluded that the current prohibitions against classification and those relating to the continuation of classification of information not requiring protection in the interest of national security are sound policy and should be included in any superseding Order. Further, that the present sanction in Executive Order 11652 is too narrow in terms of available sanctions, and is not adequate to deal with the problems of misuse of the classification system and unauthorized disclosure. Finally, the Sub-Group concluded that there does not appear to be a need for specific criminal sanctions for violations of the prohibitions. In the extreme case that an obstruction of justice is caused by a classification made for a prohibited purpose, the criminal sanction which attaches to that offense could be invoked.

OPTIONS:

1. Retain the provisions of Section 13 of Executive Order 11652 and of Section X.D. of the NSC Directive of May 17, 1972.

ADVANTAGES:

Under this option Departments could continue present practices and systems for enforcement of compliance with the operable provisions of the classification system.

DISADVANTAGES:

a. This option allows for only a single relatively weak sanction which becomes operative only for "repeated abuse."

b. This option does not provide for specific sanctions or a range of sanctions for unauthorized release or disclosure of classified information.

c. Classification and continuation of classification in violation of the Order are not explicitly subject to administrative sanction under this option.

2. Include in the Order provisions for administrative sanctions for *willful origination or continuation of classification of information in violation of the Order or an implementing Directive; willfully releasing or disclosing or causing the release or disclosure of classified information in a manner not authorized by the Order or an implementing Directive; or other violations of the Order as determined by the head of a Department. Heads of Departments will specify the provisions of the Order and implementing Directives for which violation is subject to administrative sanctions, and will specify the applicable schedule of sanctions in accordance with the major purposes of the Order and the particular requirements of the Departments.

ADVANTAGES:

a. This option places proper emphasis on the importance of strict compliance with Executive order standards and criteria for classification, declassification and disclosure.

b. The strict compliance with classification standards and criteria which would result from this option would probably result in the generation of less classified material, earlier declassification of that information, and more and earlier public availability of information concerning the affairs of Government.

c. Administrative sanctions can be imposed more promptly and more surely than criminal sanctions and at lower cost to the Government.

d. Responsibility for enforcement by use of administrative sanctions will be in the heads of Departments, the officials to whom the Order delegates authority for classification and responsibility for protection of classified information.

DISADVANTAGES:

a. Departments will be required to revise regulations pertaining to enforcement of compliance with the Order and implementing Directives and to revise security education and training activity and materials.

* The Sub-Group contemplates that the term "willful" would be defined, or that the Order would be drafted in such a manner that specific intent could be inferred by a requisite degree of negligent type conduct.

b. This option would probably result in a lack of uniformity among Departments in the application of sanctions.

3. Include in the Order provisions for a range of sanctions, e.g., reprimand, suspension without pay, removal, which may be imposed for Option 2 abuses or violations in accordance with applicable law and Departmental regulations.

ADVANTAGES:

a. This option would tend to ensure the uniform application of sanctions among the Departments.

b. This option would provide a range of sanctions.

DISADVANTAGES:

Departments will be required to revise regulations pertaining to enforcement of compliance with the Order and implementing Directives and to revise security education and training activity and materials.

4. Include in the new Executive order a section which will require all government employees to execute a secrecy agreement as a condition of obtaining or continuing access to classified information.

ADVANTAGES:

a. Has educational value

b. Will serve as a deterrent.

c. Will allow the Government to seek a civil injunction to prevent the disclosure of classified information.

DISADVANTAGES:

a. The administering of the program may outweigh its benefits.

b. The Government's ability to seek an injunction would probably prove useless in most instances because it would not have prior knowledge of the planned disclosure.

c. Most employees would probably find the requirement of signing such an agreement insulting and demeaning.

5. Include in the new Executive order a section which will require the use of a uniform secrecy agreement whereby they agree not to publish, disclose or otherwise make available classified information to any unauthorized person and that all government employees execute such an agreement as a condition of obtaining access to classified information.

ADVANTAGES:

a. Same as Option 4

b. Added advantage of reducing legal problems in attempting to enforce the agreement because of its uniformity.

DISADVANTAGES: Same as Option 4.

6. Include in the new Executive order a section which will require all government employees to execute a secrecy agreement as a condition to obtain employment or continuing in their present employment.

ADVANTAGES: Same as Option 4.

DISADVANTAGES: Same as Option 4 but has added disadvantage that it could present legal problems in attempting to apply it to the military, career civil service entrants and present government employees.

7. Include in the new Executive order a section which will require all government employees to execute a secrecy agreement as a condition of obtaining access to classified information, with a provision calling for liquidated damages or a civil fine.

ADVANTAGES: Same as Option 4 but also adds two additional deterrents through the liquidated damage clause or a civil fine requirement.

DISADVANTAGES: Same as Option 4. Also has the disadvantage that any provision calling for a civil fine could not be mandated by an Executive order, and would require legislation. While legislation would not be necessary in the case of a liquidation damage clause, such a clause would prove awkward to enforce because of the difficulty of placing a value on the classified information disclosed.

RECOMMENDATIONS: It is the consensus of the Sub-Group that there be included in the new Executive order sections which would incorporate provisions as set forth in Option 2 and in Option 3. Further, that a section be included requiring all government employees to execute a uniform secrecy agreement as a condition of obtaining access to classified information, as set forth in Option 5. Additionally, that the new Executive order should continue to direct that violation of relevant criminal statutes, e.g., 18 USC 793, 794 and 798, be referred promptly to the Department of Justice for investigation and for prosecution as appropriate.

ISSUE: How unnecessary and duplicative practices and procedures can be eliminated, reducing expenses.

DISCUSSION: In addressing this issue, it was agreed at the outset that any options and recommendations which might evolve from the Sub-Group's deliberations would not be based on cost reduction exclusively. Rather, care would be exercised to assure no significant lessening of security or, alternatively, to assure in any event an acceptable level of risk.

Primary emphasis was placed on an examination of the need for standardizing existing investigative requirements for determining trustworthiness as well as the positive and negative aspects of "compartmentalization." More specifically, the Sub-Group considered: (1) Executive Branch guidelines for determining trustworthiness; (2) Executive Branch guidelines for establishing compartments or special access programs; (3) standard procedures for access to compartmented classified information; and (4) the numbers of people requiring access to various levels of classification and the feasibility of reducing such numbers to the minimum consistent with operational requirements and needs.

Although there may be differences among the Sub-Group participants there are a number of concepts or premises upon which there is a general consensus. Among them are the following:

-- The levels of classification represent levels in degree of sensitivity. Those may be related to degrees of acceptability of risk, which in turn may warrant differences in various aspects of a security program, including scope of investigation, adjudication standards and criteria, and resolution of doubt.

-- Degree of risk, and the acceptability thereof, may vary not only according to the level of classified information but also according to the frequency of access and the attendant control procedures.

-- The differences between suitability for employment in general and trustworthiness for security clearance are usually manifold and so profound as to constitute a generic distinction rather than mere differences in degree. Unless access to classified information is so inextricably involved in the very nature of a position, the decision concerning security clearance must be considered separately from the decision concerning employment.

-- A position may be sensitive in terms of the national security for reasons other than requiring access to classified information.

-- Although costs theoretically should not constrain security procedures deemed necessary, in actual practice they do. These and other factors dictate that the numbers of persons cleared for access to classified information be held to the minimum necessary and that the process of clearance be made as cost-effective as practicable.

-- There is value in uniformity among agencies, in both investigative and adjudicative standards for like sensitivity levels.

-- Agencies may have different personnel information needs, some of which may not be directly related to clearance for access to classified material.

-- The efficacy of sources of personal background information may vary over time, e.g., as public attitudes evolve, as privacy concepts gain acceptance, or even as memories fade.

-- Analytical studies of the effectiveness of sources and scope of investigation have been conducted by individual agencies and, while some have resulted in tentative conclusions, few, if any, have yet gained unqualified acceptance among the community of security specialists.

-- Some types of information of high sensitivity, such as certain kinds of intelligence material e.g. Sensitive Compartmented Information (SCI), certain aspects of operational plans and certain information concerning operational systems, may require special restrictive physical and procedural safeguards.

The current Order requires: "No person shall be given access to classified information unless such person has been determined to be trustworthy ..."(Sec.6(A))." The accompanying NSC Directive explains: "No person shall be given access to classified information or material unless a favorable determination has been made as to his trustworthiness. The determination of eligibility, referred to as a security clearance, shall be based on such investigations as the Department may require in accordance with the standards and criteria of E.O. 10450 and E.O. 10865 as appropriate."

E.O. 10450, which prescribes standards and criteria for all Federal civilian employment, including the sub-set of persons having access to classified information requires that the scope of investigation shall be determined in the first instance by the relationship of the position to the national security. Access to classified information of any

sort makes the position sensitive. That Order does not recognize degrees of sensitivity other than sensitive (requiring a complete background investigation conducted in person by trained investigators) and non-sensitive (requiring at least a National Agency Check and written inquiries (NACI).

The President directed in 1965 that the Civil Service Commission make certain changes in the program. Among these changes was one that distinguished two types of sensitive position, (1) critical-sensitive which includes access to Top Secret information (as well as certain other policy-making criteria not directly related to classified information) and (2) noncritical-sensitive, which includes access to Secret or Confidential information. The full field investigation was retained as the required coverage for critical-sensitive positions but the coverage for noncritical-sensitive was reduced, as a minimum, to the NACI, the scope previously required for non-sensitive. Agency heads are permitted to expand this minimum coverage on any employee, however, when such action is considered "appropriate."

None of the various laws authorizing agency action in matters of personnel security, such as P.L. 81-733 (5 USC 7311), or the National Security Act (50 USC 403), provides any more specific guidance concerning the scope of investigations or the method of conducting them. The lack of specificity has allowed the development of a wide variety of investigative coverage among the various agencies, in terms of both years covered and types of source contacted.

In order to highlight the variance in investigative coverage among the Departments, it is well to compare the investigative practices and procedures of the Department of Defense which Department meets the minimum requirements of E.O. 10450 for determining trustworthiness and the practices and procedures of the Central Intelligence Agency (CIA) which conducts more comprehensive investigations for the same purpose.

The investigative scope used by the CIA in conducting investigations on their employees includes, as a minimum: (1) verification of date and place of birth and citizenship; (2) check of the subversive and criminal files of the FBI (includes National Agency Check as appropriate); (3) check of appropriate police records back 15 years; (4) verification of financial status and credit habits back 5 years; (5) neighborhood check back 5 years; (6) confirmation of employment back 15 years; (7) verification of attendance at educational institutions back 15 years; (8) review of

appropriate military records; (9) interviews with knowledgeable acquaintances back 15 years; (10) National Agency Check of the spouse; and (11) a personal interview with the individual. The requirement for this scope of investigation plus a polygraph examination is based on CIA's considered judgment that only such procedures will provide a significantly high degree of assurance that career personnel, who are exposed to large volumes of highly sensitive material over extended periods, are indeed trustworthy.

The Department of Defense, on the other hand, has adopted investigative practices and procedures which are generally tailored to the level of sensitivity to which an individual may require access in the performance of his official duties. For example, the investigation used by the Department for determining trustworthiness for access to the highest level of sensitivity (Top Secret), is similar to the CIA investigation, above described, except that the scope is normally 5 years, as contrasted to 15, and there is no investigation of the spouse. For military personnel, the Department has accepted as a measure of trustworthiness for access to Top Secret ten years continuous honorable active duty plus a National Agency Check (NAC). With respect to those individuals requiring access to Secret and Confidential information, a NACI is generally the acceptable investigative standard for civilians and a NAC for military. Notwithstanding, there are some practical waiver considerations. For example, a company under contract to any Department or Agency involved in the Industrial Security Program may grant access to Confidential information related to the performance of that contract without a NAC.* (There are 16 Departments and Agencies of the Executive Branch participating in the Industrial Security Program). It is the Department of Defense view that its investigative practices and procedures for determining trustworthiness are practical, cost-effective and productive. Notwithstanding, there were differences of opinion among the Sub-Group members on whether the exclusive use of a NAC constitutes an effective investigative technique for determining trustworthiness.

In addition to the standard DoD investigative practices and procedures, above described, there are more restrictive investigative requirements imposed on the DoD by the Director of Central Intelligence for determining trustworthiness of DoD personnel requiring access to Sensitive Compartmented Information (SCI). These involve the conduct of a Special Background Investigation similar in scope to that conducted for employment in CIA. In the DoD, this investigative requirement is applicable to approximately 114,000 Defense personnel and necessitates the allocation of over 50% of the Department's investigative resources to clear only 10% of the total DoD personnel requiring clearance for access to classified information. The problems of the DoD in meeting

* See attached appendix for background and cost impact.

these added investigative requirements are compounded by the fact that Congress directed a FY 76 cut in the Defense Investigative Service personnel spaces of 664 out of a total of 2,470. Moreover, the Congress is continuing close scrutiny of the entire Executive Branch personnel investigative effort.

Other Departments and Agencies of the Executive Branch which conduct investigations to gain data on which to base a determination of trustworthiness utilize different scopes of investigation for different levels of access which vary between the minimum requirements adopted for Defense use and the maximum for CIA use. The costs expended by each Department for the single purpose of determining trustworthiness for access to classified information are commensurate with the techniques employed. For example, cost to the government for a NAC conducted by the Department of Defense for determining access to Confidential and Secret material is approximately $10. Cost for a DoD background investigation (5-year scope) for determining access to Top Secret is $325 and that for access to SCI (15-year scope) is $395. This compares with a cost of approximately $1,000 for a background investigation conducted by the Federal Bureau of Investigation or approximately $700 by the Civil Service Commission. It is apparent that any determination to standardize investigative and adjudicative procedures must consider the cost impact of such a move. A decision to broaden the scope to require a full field investigation on just those DoD personnel currently cleared on the basis of a NAC would result in a 32 fold cost increase. The question remains as to whether the expenditure representing the difference between the less restrictive treatment and the extreme is justified and whether that difference buys the U.S. any better security.

There is general consensus that investigative practices and procedures in use across the Executive Branch should not be standardized for standardization sake. Rather, any attempt to bring about standardization should have the objective of:

-- carrying out more effectively and equitably the operations of the Government's personnel investigative and security programs;

-- promoting greater uniformity in providing safeguards for the rights of individuals with due regard for the interests of the Government;

-- facilitating the reciprocal use of security clearances among agencies of the Executive Branch;

-- assuring that the adoption of such standards would involve a mutually acceptable level of risk and protection; and

-- promoting cost effectiveness

It is considered that each Department in the Executive Branch which currently employs a particular investigative security practice and procedure to accommodate its needs will have the tendency to support and fully justify its use. Under these conditions, a review of existing investigative security practices and procedures for purposes of standardization is thought to be best undertaken by an office above the Departmental level with authority to resolve any conflicts which may arise between Departments.

The scope of investigation for determining trustworthiness is, of course, only one aspect of assuring personnel reliability. An equally important aspect is that supervisors at all levels of supervision be continually cognizant of their employees' behavior in order to assure the detection of changes in habits and character which may adversely affect their status with respect to the safeguarding of classified information. In this connection, there is evidence that hostile espionage has successfully recruited personnel investigated and cleared for SCI access as well as those with collateral clearance.

The next principal area of discussion focuses on the matter of "compartmentalization."

As near as can be determined, the first use of compartmentalization occurred in the Manhattan Project. The use of compartments, in all likelihood, then spread to the area of cryptologic matters and since, the concept has been widely used in the areas of intelligence, operational planning and in the scientific and technical arena.

Compartmentation appears to come about because of the view that the total body of information involved is more sensitive, regardless of the classification level to which it is assigned, than that which is classified at the same level outside the compartment. In this connection, the view was expressed that information classified, for example, at the Secret level will cause, by unauthorized disclosure, the same degree of damage to the national security regardless of the substance. Some members took the position that within the ambit of the classification "Secret," there are gradations of sensitivity. The resolution of this matter has a bearing on the establishment of compartments.

Special access procedures are supplements to the normal administration of the classification system and are designed to provide additional means of limiting and enforcing access to and use of the information involved. They include but are not limited to such things as access lists, restricted areas, and "special clearances." Executive Order 11652 sanctions the use of such special procedures but does not establish any specific tests for such use or require periodic review and revalidation of procedures in effect.

The number of compartments currently established in the Executive Branch is not fully known. What is known is that compartments do exist and they vary widely in size and scope.

The best estimate is that in the SCI area, approximately 200,000 people are required to have an "access authorization" based on information gathered by utilization of the investigation prescribed in DCID 1/14. The Department of Defense, alone, has 114,000 people cleared for access to SCI.

Some members expressed the view that many current compartments appear to have an unreasonable number of personnel involved. Thus, the question remains whether those compartments wherein access is permissive to such large numbers of personnel serve the intended purpose of limiting dissemination to the minimum number of persons having an absolute need-to-know. Also to be resolved is the question of whether those people who have an immediate need for SCI or other compartmented information and who have been found trustworthy through a Background Investigation, are unduly inhibited in performance of their official duties because they are not certified for access to those compartments.

Some believe that the widespread use of compartments and the stringent access controls associated with them has inadvertently denied high level officials in the Executive Branch information which may be needed by them to develop viable options in their wide areas of functional responsibility. They also encounter problems in initially identifying the compartmented areas and the substance of them due to the fact that there are few, if any, central offices in which the compartments are recorded and described. For example, if the President needed immediate information concerning a particular subject matter which information may be compartmented, his staff would be hard pressed to identify the compartment in which the information is contained.

Time constraints did not permit the Sub-Group to fully explore all aspects of the physical safeguarding procedures and practices which are designed to protect information against unauthorized disclosure. The members did consider the feasibility of reducing the

numbers of people which have been determined to require access to various levels of classification to the minimum consistent with operational requirements and needs. In this connection, there was consideration of need for a provision for requiring that heads of departments assure that a demonstrable need for access is established prior to the issuance of clearances.

OPTIONS: FOR DETERMINING TRUSTWORTHINESS

OPTION 1:

Continue to permit heads of Departments of the Executive Branch to determine scope of investigation, in conformance with Executive Order 10450, for purposes of determining trustworthiness of individuals for access to classified information.

ADVANTAGES:

a. No additional Presidential action required.

b. No need to issue new Executive Branch regulations.

c. Each department/agency retains flexibility.

d. Not necessary to reeducate/retrain implementing personnel.

DISADVANTAGES:

a. E.O. 11652 does not establish procedures for determining trustworthiness.

b. Some investigative scopes contain redundancy and duplication.

c. Some investigative scopes are very expensive.

d. Reciprocal acceptance of clearances will be jeopardized.

e. Acknowledges inability of Executive Branch agencies to agree on investigative standards.

f. Individuals having access to the same degree of sensitivity of classified information will continue to be investigated to different degrees in the various agencies of the Executive Branch.

g. With respect to military personnel, investigative agencies lack a clear Presidential mandate, required by the Privacy Act of 1974, to collect criminal history record, education, credit and other similar record information required to make a personnel security determination with respect to access to classified information.

OPTION 2:

Designate an office in the Executive Office of the President to develop and promulgate standards for uniform application across the Executive Branch for scope of investigation and for adjudication of results, including due process safeguards, to determine trustworthiness of individuals for access to TOP SECRET, SECRET and CONFIDENTIAL information regardless of its substance.

ADVANTAGES:

a. Decision establishing the standard will be made above Department/Agency level thus eliminating parochialism.

b. Uniformity will be achieved in all Departments/Agencies.

c. Simplify administration.

d. More effective utilization of investigative resources.

e. Enhances public understanding and acceptance of Federal Personnel Security Program.

f. Avoids criticism of current procedures under which trustworthiness for Top Secret is not accepted for access to compartmented information.

g. Reciprocity of clearance will be assured.

h. Investigative standards will be limited to three (one each for Confidential, Secret and Top Secret).

i. Relates investigative procedures to the three levels of sensitivity (i.e., Confidential - minimum level investigation, Secret - intermediate level investigation and Top Secret - maximum level investigation.)

DISADVANTAGES:

a. Does not recognize the long-standing policy assigning compartmented information a higher level of sensitivity than Top Secret.

b. Denies individual Department/Agency flexibility.

OPTION 3:

Designate an office in the Executive Office of the President to develop and promulgate standards for uniform application across the Executive Branch for scope of investigation and adjudication of results, including due process safeguards, to determine trustworthiness of individuals for access to SECRET and CONFIDENTIAL (one standard) and TOP SECRET (another standard).

ADVANTAGES:

Option 3 has substantially the same advantages as Option 2 except that there will be only two standards for determining trustworthiness.

DISADVANTAGES:

Option 3 has substantially the same disadvantages as Option 2; additionally, it requires the same level of trustworthiness for SECRET and CONFIDENTIAL although they are two distinct classifications.

OPTION 4:

Designate an office in the Executive Office of the President to develop and promulgate standards for uniform application across the Executive Branch for scope of investigation and adjudication of results, including due process safeguards, to determine trustworthiness of individuals for access to SECRET and CONFIDENTIAL information (one standard), TOP SECRET (another standard), and especially sensitive information within the ambit of TOP SECRET (a third standard).

ADVANTAGES:

a. Decision establishing the standard will be made above department/agency level thus eliminating parochialism.

b. Uniformity will be achieved in all departments/agencies.

c. More effective utilization of investigative resources.

d. Reciprocity of clearance will be assured.

e. Will assure that the most sensitive information (intelligence sources and methods and other currently compartmented information) will be afforded the highest security standard without establishing a new level of classification.

f. Compartmented information currently classified CONFIDENTIAL and SECRET will no longer require the highest level investigation thus significantly reducing investigative costs.

g. Cost savings will be further achieved by not requiring the highest level of investigation for that TOP SECRET information which is not currently compartmented.

DISADVANTAGES:

a. Ignores the three level classification system.

b. Tends to downgrade the sensitivity of regular TOP SECRET information.

c. A new two level TOP SECRET trustworthiness standard (including a "super" TOP SECRET) would confuse both the public as well as government personnel and could invite criticism from both the Congress and the press.

d. Complicates the investigative process for TOP SECRET by requiring two separate investigative scopes for TOP SECRET.

e. Complicates the adjudicative process for TOP SECRET by requiring two separate clearance standards for TOP SECRET.

f. Requires the same level of trustworthiness for SECRET and CONFIDENTIAL although they are two distinct classifications.

NOTE: If Option 2, 3 or 4 is adopted, it would be understood across the Executive Branch that once an individual is cleared for access to a particular level of classification, that clearance would be reciprocal among agencies.

OPTION 5:

Same as Option 2 through 4 except that all Confidential clearances under the DoD Industrial Security Program would be granted by the government.

ADVANTAGES:

a. Uniformity would be achieved in that all individuals, contractor and government, would be cleared at the Confidential level on the same investigative basis.

DISADVANTAGES:

a. Would create a significant disruption in defense contractor facilities, resulting in costly delays in contract performance, because new employees could not be utilized on Confidential work for over two months after they are employed and brought on board. The Government would incur additional liability to its contractors in that contract overhead costs would increase in a range of $120 million to $180 million annually.

b. The change would invoke the ire of industry and be criticized as increased bureaucratic involvement in the private sector. It would significantly impinge upon industry's ability to perform contracts in an effective, efficient and timely manner.

c. Increase the security clearance workload of the DoD Industrial Security Program approximately 50%.

d. Would place an additional investigative burden on the Defense Investigative Service.

OPTION 6:

Same as Option 2 through 4 except that Confidential clearances would continue to be granted by the Contractor.

ADVANTAGES:

Converse of Disadvantages under Option 5.

DISADVANTAGES:

Converse of Advantages under Option 5.

OPTION 7:

Same as Option 2 through 4 except that the standards would be established in the new Executive Order.

ADVANTAGES:

a. Places the full authority of the Presidency in support of standardization.

b. With Presidential authorization, investigative and adjudicative procedures would be less vulnerable to legal challenge.

c. With Presidential authorization, investigative agencies would have a strong legal basis for collecting criminal history records, eduction, credit and other similar information required to make personnel security determinations.

DISADVANTAGES:

a. Difficulty of change once the new Order is issued.

b. Would add to the length of the Order.

c. If the Order were to detail investigative and adjudicative standards, the difficulty in obtaining interagency agreement would delay issuance of the Order significantly.

d. Existing problems in the conduct of traditional personnel security investigation requires thorough research and analysis, developed in coordination with all major departments, before specific details are locked in an Executive Order.

OPTIONS: FOR COMPARTMENTATION

OPTION 8:

Continue to permit heads of Departments to make special departmental arrangements for compartmentation as provided for in Section 9 of Executive Order 11652.

ADVANTAGES:

a. Maintains continuity with current practice.

b. Permits sensitive information to be protected by means supplemental to those provided by the classification system alone.

DISADVANTAGES:

a. Provides no uniform criteria against which system compliance with national security objectives can be monitored.

b. Continues the high costs, both in terms of resources and of limits on availability and use of information, inherent in the present large number of wide-ranging special access procedures.

c. Perpetuates present variations between procedures on extent of access and use restrictions for information of comparable sensitivity.

d. Gives no positive assurance that special access procedures will be kept up-to-date.

OPTION 9:

Eliminate all compartments in the Executive Branch of government and in their place provide in the Executive Order for strict enforcement of the need-to-know principle by placing responsibility on the custodian to determine that the intended recipient has a need-to-know and has been determined to have been found trustworthy.

ADVANTAGES:

a. Simplifies the administration of the system to protect national security information, by making clearance and need-to-know the sole criteria for access to any protected information.

b. May broaden working level access to information heretofore denied it.

DISADVANTAGES:

a. Fails to recognize that there is some information which is of such sensitivity that access to it must be strictly limited, beyond the extent achievable through normal safeguarding procedures.

b. Denies senior national security officials a means to enforce very limited access for sensitive information of high-level concern.

c. Would likely prompt the use of informal arrangements to restrict access, thus undermining faith in the system.

d. Would, in some cases, be in violation of agreements with allies calling for the protection of specified information by special access controls.

e. Risks foreign sources of intelligence refusing to cooperate with the U.S. for fear that our system would be unable to protect their identity and working relationship.

OPTION 10:

Establish standards for the creation or continuation of compartments or special access programs. Such standards would require that all special access programs be created or continued only by the authority of a head of a Department, personally and in writing. Moreover, such special access programs shall be created or continued only on the specific showing that:

(1) Normal safeguarding procedures are inadequate to protect the information.

(2) The size of the compartment (numbers of people requiring access) is reasonable and is limited to the absolute minimum.

(3) The special access controls balance the need to protect the information against the full spectrum of needs to use the information.

(4) Further, all such special access programs shall automatically terminate after three years unless renewed in accordance with the above procedures.

ADVANTAGES:

a. Permits supplemental protection of very sensitive information within the bounds of the classification system.

b. Should reduce the number and extent of current special access programs, thereby better protecting that which remains within such programs and generating cost savings.

c. Insures, through very senior-level review and approval, that the respective needs for protection and utility are fully balanced. In the process, helps national security planners to be more aware of what information is available through what channels.

d. Insure that special access programs are regularly reviewed, and kept up-to-date or cancelled as circumstances dictate.

e. Provides uniform criteria against which departmental compliance can be monitored.

DISADVANTAGES:

a. Will involve effort in re-examining and possibly changing existing special

b. Will require some additional effort in periodic reviews.

OPTION 11:

Require that special access programs be created only by authority of the National Security Council and/or the DCI (as appropriate) under the same criteria as in Option 8 above.

ADVANTAGES:

a. Permits supplemental protection of very sensitive information within the bounds of the classification system.

b. May reduce the number and extent of current special access programs.

c. May help the highest level of national security planners be more aware of what information is available through what channels.

d. Should insure that special access programs are reviewed and kept up-to-date.

DISADVANTAGES:

a. Will require the most senior U.S. national security forum to involve itself in administrative matters that can be better adjudicated at the departmental level.

b. May result in uneven protection for very sensitive information, because the extremely senior review and approval level may not have time to consider all pertinent aspects of proposed programs.

c. Undercuts the responsibility of department heads for determining what information requires protection.

d. Divides responsibilities of whatever oversight office for the information security program is created by the new Executive Order between the NSC/DCI and that office.

OPTION 12:

Include in the new Order provisions which require that heads of Departments:

a. Take action necessary to insure that number of people granted access by his Department to each level of classification be reduced to and maintained at the minimum consistent with operational requirements and needs.

b. Assure that a demonstrable need for access is established prior to initiation of action required for any clearance for access to classified information after the effective date of the new Order.

ADVANTAGES:

a. Will insure that access to classified information is limited to the minimum numbers of persons necessary thus reducing the risk of compromise.

b. Strict enforcement will bring about cost avoidance.

c. Strengthens the "need-to-know" principle.

DISADVANTAGES: None.

OPTION 13:

Include in the new order a requirement that heads of Departments cause a continuing review of safeguarding practices and procedures with a view to eliminating those which are found to be duplicative and unnecessary.

ADVANTAGES:

a. Consistent with mandate of PRM/NSC-29.

b. Effective implementation should result in cost reduction without loss of security.

c. Effective implementation should result in simplification.

DISADVANTAGES: None.

OPTION 14:

Include a specific provision in the Order which would authorize the obtaining of criminal justice information from Federal, State, and local law enforcement agencies as an integral part of the scope of investigations required for determining trustworthiness pursuant to the Order.

ADVANTAGES:

a. Establishes Executive Order authority for the collection of such information.

b. Diminishes possibility of legal challenge to the collection and use of such information.

c. Should have a favorable effect on the shaping of state and local statutes and policies with respect to release of such data.

d. Would serve to rectify the misunderstanding currently existing at state, local and institutional level as to the authority for, need and use of such data.

e. Would serve as a basis for revision of LEAA regulations relating to criminal history records which would further enhance state and local agency cooperation.

DISADVANTAGES: Same as Option 7.

NOTE: This option was introduced by one department and not considered in group deliberations. Supporting rationale is presented at the asterisk below.

RECOMMENDATION:

Concerning the trustworthiness options, there appears to be consensus that if standardization of scope of investigation and adjudication practices is brought about, it would be through the adoption of Options 2 thru 4 rather than by prescribing standards in the new Order as outlined in Option 7. Notwithstanding, there appears to be a clear consensus in the intelligence community to adopt Option 1 (status quo).

Concerning the compartmentation options, the consensus of the group is to favor Option 10. There appears to be consensus in favor of Options 12 and 13.

*The Privacy Act of 1974 prohibits the release of certain personal information unless the requirement for such information is grounded on statutory or Executive Order authority. Exceptions in the statute have been made, however, with respect to law enforcement agencies. Unfortunately, the term "law enforcement agencies" does not reach to Executive Branch organizations which are engaged primarily in the collection of personal data required to make personnel security determinations. The Law Enforcement Assistance Agency has issued regulations which were intended to facilitate the collection of such required personal data by non-law enforcement agencies requiring the data for personnel security determinations. However, in the absence of specific enabling language set forth either in public law or Executive Orders, there has been considerable misunderstanding at state, local and institutional levels with respect to the authority to collect, and the need for, and use of such information by non-law enforcement agencies conducting essentially personnel security investigations. Clearly establishing the requirements of the Executive Branch for such information in an Executive Order would facilitate the collection of this personal data which is vital to the adjudicator in making personnel security determinations.

Company Granted Confidential Clearances
Background and Cost Impact Data

In the early 1950s, the concept was introduced which permits the contractor to issue Confidential clearances to other than Top Management personnel. The procedure was needed so as to permit industry to immediately utilize the services of new employees on Confidential work, avoiding the delays encountered in connection with a normal Government investigation for issuance of clearance. Additionally, this procedure provided significant relief to the already overtaxed investigative resources of the Department of Defense.

The theory which supports the concept is that the contractor, in conjunction with the normal preemployment screening, will develop pertinent information concerning the individual. The contractor is precluded from issuing a Confidential clearance if he becomes aware of any information which would indicate that clearance is not "clearly consistent with the national interest." Additionally, the employee must execute a form, answering certain questions pertinent to clearance. Where these questions raise an issue with regard to credibility, again the contractor may not issue the clearance, and the case must be referred to the Department of Defense.

The current national trend of providing better protection to individual privacy is making it increasingly more difficult for employers to conduct preemployment inquiries and this, in turn, reduces the effectiveness of preemployment screening.

In the mid-1950s, a pilot test was conducted. Fifty thousand company-Confidential clearance cases were selected at random and National Agency Checks were conducted. As a result of an analysis of these 50,000 cases, it was determined that reliance on the contractor's normal employer-employee relationship as the basis for the issuance of a Confidential clearance was sound from a security standpoint. Hence, the program has been continued.

It has been variously estimated that if a new employee is hired to perform on classified work, it will cost the contractor between $50 and $70 a day for each day a security clearance request is pending, since the employee cannot be fully utilized without having access to classified information. On the basis of estimates that approximately 60,000 new company-Confidential clearances are issued each year, indirect cost to the Government in the form of contract overhead would result in an annual expenditure of between $120 million and $180 million per year, if the company-Confidential clearance concept were to be discontinued.

Appendix

In addition, there would be an increased work load of approximately 50 percent in the number of cases now handled by the DoD Industrial Security Program. First year costs would be significantly higher for Government processing and investigations, because there are approximately 300,000 contractor personnel currently cleared with company-Confidential clearances.

ISSUE: Which information requires protection and for how long and what criteria should be used in making this judgment.

DISCUSSION: So much of the assigned issue which concerns how long information should be protected was not addressed by this Sub Group. That matter is being considered by the Sub Group reviewing the issue of how to promote increased public access to information no longer needing classification through a more rapid and systematic declassification program, Sub Group C/D-3.

In its deliberations, the Sub Group considered a wide range of factors related to the issue involved. These included but were not limited to: need for expression of specific criteria for classification; need for expression of absolute prohibitions against classification of certain information or for certain purposes; re-examination of the scope of the term "national security"; need for revision of the classification categories; usefulness of paragraph classification marking; and usefulness of classification guidelines as a means for achieving uniformity in classification.

In considering whether the three categories of classification, i.e., Top Secret, Secret, and Confidential, as established by E.O. 11652 are adequate, the view was expressed that these categories are now well recognized throughout the United States Government, defense industry, and in the international community. It was also concluded that it was inadvisable to consolidate the three categories into two because that would result not in appreciably less classification, but rather in information previously classified as Confidential merely being classified as Secret. Also rejected was the idea that the Executive Order permit Department and Agency heads to adopt a fourth category of information which could be protected on grounds other than national security, such as, for example, that unclassified information now categorized under Departmental regulations as "FOR OFFICIAL USE ONLY" and "LIMITED OFFICIAL USE." It was felt that this body of material does not belong in an Order dealing with national security information and could create the impression that the government was seeking to protect more information in a new Order than under E.O. 11652.

Also considered was the language of the test for assigning information to a classification category. That test is that the unauthorized disclosure of the information involved could reasonably be expected to cause a degree of damage to the

national security. It was the consensus of the Group that this test has withstood examination in the courts and there appears to be no need for changing it. However, some members felt it might be appropriate to include language in the new Executive Order which would make clear that, in order to classify information, the classifying authority must satisfy himself that more than a modicum of damage could reasonably be expected from unauthorized disclosure. A suggested way to accomplish this would be to modify the definition of the standard for Confidential by including words such as "appreciable," "significant," or "demonstrable."

With respect to the collective term, "national security," as used in E.O. 11652, i.e., "the national defense or foreign relations of the United States," the Group considered whether the scope of that term should be expanded. Some consideration was given to the need for including in the term "national security." in addition to information concerning foreign relations and national defense, information concerning other subject matters which might be considered as deserving protection against unauthorized disclosure such as, for example, information concerning terrorist activities, narcotics, trade secrets, etc. The view was expressed that to the extent that any subject matter information is information concerning national defense or foreign relations, it is within the ambit of the term "national security" and, to the extent that unauthorized disclosure of such information would cause damage to the national security, may be classified and afforded protection in accordance with the present Order. It was further viewed that any information concerning such things as narcotics or terrorist activities which does not also concern national defense or foreign relations would not qualify for security classification protection in the interest of national security. The observation was made that some narcotics or terrorist information, not protectable pursuant to the Executive Order, might qualify under the terms of the Freedom of Information Act or other statutes for protection or withholding from public release. In connection with this matter, the question was also raised as to whether the President's constitutional authority to protect information in the interest of national defense and foreign relations could be extended to protect information not related to those governmental functions. Resolution of this question was not undertaken by the Sub Group.

Considered at great length was the matter of whether a new Order should require that classification of decisions by the Executive Branch weigh the relative merits of public disclosure of the information against the interests of national security. Some members had reservations concerning inclusion of a "balancing test" in a new Executive Order. The basis for this concern appeared to be that original classifiers who are well qualified to arrive at determinations based upon damage to the national security alone, may not be equally qualified to consider the advantages of public disclosure. Moreover, the view was expressed by some members that the courts, in adjudicating whether a classification complies with the Order, would demand that the government give a clear showing that the "balancing test" was made in each and every case where original classification is involved. This could adversely affect the presumption in favor of classification protection that the government generally enjoys in Freedom of Information Act litigation. Others expressed the view that the inclusion of the "balancing test" in an Executive Order should lead to more careful classification decisions and might, in fact, result in reducing unnecessary classification, thereby making more information available to the public.

The Group examined the need for the Executive Order to express specific criteria for classification. Executive Order 11652 does not include such criteria but does provide examples of the kinds of information which qualify for protection against unauthorized disclosure in each of the two highest classification categories; Secret and Top Secret. In a new Executive Order, the expression of specific classification criteria would be in lieu of the examples and would apply to all information concerning national defense and foreign relations. For example, information would be classified if its disclosure would "weaken the position of the United States in the discussion, avoidance or peaceful resolution of potential or existing international difficulties" and thereby cause some degree of damage. The criteria would be broad enough to cover information legitimately protectable but would be more explicit than the existing examples. It was the opinion of some that the criteria could be treated as merely illustrative in which case examples could be incorporated in the categories of classification. Others felt that the criteria could be exclusive. In the later case, before information could be classified, an original classifier would have to establish that the information fell within one or more of the criteria and that its disclosure would meet the test of one of the levels for classification.

The Sub Group also considered the matter of whether the new Executive order should go beyond Executive Order 11652 in prohibiting classification of information for certain reasons, e.g., to cover up the commission of a crime. The Sub Group concluded that such additional prohibitions are desirable. A member believes that the Order should go further and mandate public disclosure of certain types of information which, by statute, e.g., War Powers Act, are now required to be disclosed. Others were opposed to this view on the basis that this Executive order is not the appropriate vehicle for such provisions and, further, that the statutes do not prohibit the classification of certain elements of these categories of information. An expression was made that the promulgation of public disclosure policy is not the major purpose of this Order.

Although not directly related to the main issue, some discussion centered upon the utility of requiring that portions of classified documents, e.g., paragraphs, be identified as to the classification level of each such portion. Executive Order 11652 recommends, but does not require, that portions of classified documents be marked to show the classification of the information contained in each or that such information is not classified. Such marking is left to the discretion of the head of the Department. Some Agencies, notably, DOD, require paragraph by paragraph classification marking and believe that the practice has served to reduce the proliferation of classified information, reduce overclassification, simplify declassification, and is not unduly expensive or burdensome when compared to those benefits. Others, who have not employed the practice, believe that identifying classified portions of a document is inappropriate, misleading, or unnecessary in certain areas. It was noted however that the lack of uniformity with respect to paragraph marking throughout the Executive Branch does cause difficulty in Departments and Agencies which do require paragraph marking because the latter cannot incorporate into their system with precision and confidence information contained in documents not so marked.

The existing Executive Order is silent as to whether Departments should prepare and publish general guidance for the classification of particular subject matters. Discussion brought out that the publication of guidelines by some agencies, notably DOD and ERDA, has been found to be effective to avoid

overclassification and to achieve uniformity in classification decisions. The observation was made that in such general areas as foreign relations, intelligence and military operations, the formulation of security classification guidelines for general application is difficult and hence, relatively expensive. Participants who are particularly concerned with these functional areas questioned whether the effort to produce such guidelines is worthwhile. The consensus of the group is that the new Executive order should mandate the preparation and use of general classification guidelines, and encourage departments to amplify such with more specific guides.

The existing Executive order makes provision (Section 9) for "special departmental arrangements" with respect to access, distribution and protection of classified cryptologic material. The arrangements are in fact promulgated by national authority (National Security Council and DCI Directives) and include specific guidelines for special access, distribution and protection of such material. The present Order does not specifically make reference to the provisions of certain statutes, e.g., 18 U.S.C. 798, which single out classified cryptologic material from other classified material as particularly sensitive. Concern is expressed that such material may be disclosed inadvertantly due to a misunderstanding of the purpose and effect of the automatic declassification provisions of the Order. This concern is based on evidence that, in several instances, there have been disclosures of still classified cryptologic material by former government officials because of such misunderstanding. The opinion was expressed that a new Order should focus attention on the sensitivity of this body of material by including a reference to statutes which expressly recognize the sensitivity of such classified material.

The Sub Group felt that it was important to protect foreign government classified documents and information as well as any information and material provided to the United States in confidence by foreign governments or any other foreign sources. The present Order provides, in section 4(C), that foreign government classified information shall either retain that classification or be afforded equal protection under our classification system. Under section 5(B)(1) of the present Order, information provided in confidence by a foreign government may be exempt from automatic declassification. This latter provision implies that because information is provided in confidence it may be classified. Some felt that this implication should

be made specific in the new Executive order and further, that some unique "identifier" should be prescribed for application to this type of material. Others felt that the provisions of the present Order provide desirable flexibility which will permit classification and protection in any instance that unauthorized disclosure of information provided the United States or of the circumstances of its acquisition, would cause damage to the national defense or foreign relations.

OPTION 1:

Expand the term, "national security" as now used in E.O. 11652 to include specifically information concerning terrorist activities, narcotics, and perhaps, threats to the orderly process of government (favored by FBI).

ADVANTAGE:

Would explicitly recognize that such information is classified under the Order.

DISADVANTAGES:

a. Creates impression of expanding the scope of the Order.

b. May result in classification of information as "national security information" that should not be protected under this system raising political, and perhaps constitutional questions.

OPTION 2:

Retain the scope of the term "national security," i.e., national defense and foreign relations, as used in E.O. 11652.

ADVANTAGES:

a. Would not require reeducation process as the scope of the term is generally understood.

b. Would avoid the appearance of any attempt to encompass more information to be protected under the President's authority.

c. Would avoid the potential constitutional question concerning the limit of the President's authority.

d. The term, as expressed in the present Order, has been upheld in litigation.

DISADVANTAGE:

Would not permit information unrelated to national defense and foreign relations to be classified.

OPTION 3:

Adopt specific classification criteria which would call for the elimination of examples now included under the classification categories of Top Secret and Secret. The criteria would apply equally to all classification categories. It would be mandatory that before information could be classified, it would have to be established that the information falls within one or more of the criterion.

ADVANTAGES:

a. Would reduce the discretion of classifiers in determining whether information is classifiable.

b. Would serve as a guide to classifying authorities.

c. May contribute to minimizing unnecessary classification and ultimately to more openness.

DISADVANTAGE:

Unless the criteria are drafted with adequate foresight, subject matter which should be protected may be found to be omitted, thus precluding classification. This would require updating from time to time.

OPTION 4:

Adopt specific criteria which, in addition to examples now given under Top Secret and Secret classification categories, would be illustrative only. The criteria would apply equally to all classification categories and would constitute a basis for determining whether information is classifiable but failure of the information to meet one or more of the criterion would not preclude classification.

ADVANTAGES:

a. Same as OPTION 3.

b. An added advantage is that since the criteria are not all inclusive, information not meeting one or more of the criterion may be classified.

DISADVANTAGES:

a. Eliminates a part of the basis for classification determination.

b. May permit classification of information not requiring protection.

OPTION 5:

Retain the examples now included under the classification categories of Top Secret and Secret and possibly develop examples for Confidential without additional criteria.

ADVANTAGES:

a. Would not require reeducation process.

b. Leaves the classifier with broader discretion for determining whether particular information is classifiable.

DISADVANTAGES:

a. Does not provide adequate substantive guidance for classifiers.

b. Will permit the classification of information which does not warrant protection.

c. Does not contribute to openness.

d. Does not provide a basis for the imposition of administrative sanctions incidental to enforcement of compliance with the Order.

OPTION 6:

Require the development, use and promulgation of general classification guidelines by Departments and Agencies, and encourage them to amplify such with specific guides.

ADVANTAGES:

a. Would tend to reduce unnecessary and overclassification.

b. Would provide for consistent classification decisions.

c. Would provide standards against which to measure compliance.

d. Would assist in responding to Freedom of Information Act.

DISADVANTAGES:

a. May prove difficult to develop general guidelines for certain functional areas.

b. May be cost ineffective and non-productive in specific applications.

OPTION 7:

Make the adoption of classification guidelines in Departments and Agencies optional but encourage promulgation where practicable.

ADVANTAGES:

a. Gives the Departments and Agencies flexibility.

b. Will avoid unnecessary expenditure in those cases where the development and promulgation of guidelines are found to be cost ineffective and non-productive.

DISADVANTAGES:

a. If guidelines are not developed and promulgated, inconsistency will continue where such now exists.

b. Will not lead to standardization throughout the Executive Branch.

c. Will not provide sufficient guidance against which to measure complicance.

OPTION 8:

Do not include, in the new Order, any provisions relative to the development and promulgation of classification guidelines.

ADVANTAGE:

None.

DISADVANTAGE:

Fails to give an expression of Presidential endorsement of an administrative procedure for avoiding unnecessary classification and overclassification.

OPTION 9:

Require mandatory paragraph classification marking.

ADVANTAGES:

a. Reduces the proliferation of classified information.

b. Avoids unnecessary classification.

c. Simplifies the declassification review process.

d. Facilitates review for declassification and response to requests under FOIA and the Order.

e. Contributes to consistency and permits precision in derivative classification.

DISADVANTAGES:

a. May be viewed as administratively burdensome.

b. Will require significant education and training effort.

c. May not be generally applied to all documentary media.

OPTION 10:

Require mandatory paragraph classification marking with provision for the head of a Department to seek a waiver from an oversight body for specific classes of information.

ADVANTAGES:

a. Same as OPTION 9.

b. Has the added advantage of providing some flexibility to heads of Departments who find the practice cost ineffective or non-productive.

DISADVANTAGE:

Will not achieve complete uniformity throughout the Executive Branch.

OPTION 11:

Require mandatory paragraph classification marking with provision for the head of a Department to grant an exception for good cause for certain classes of information; require that the Department head advise in writing an oversight body of the existence and rationale for such an exception.

ADVANTAGES:

a. Same as OPTION 10.

b. Has the added advantage of providing some flexibility to heads of Departments who find the practice cost ineffective or non-productive.

c. Paragraph marking is a matter of program management and may not be appropriate for approval by an oversight body.

DISADVANTAGE:

Will not achieve complete uniformity throughout the Executive Branch.

OPTION 12:

Paragraph classification marking would be required to the extent practicable as provided in E.O. 11652.

ADVANTAGES:

a. Would not impose any additional administrative burden.

b. Maintains status quo.

DISADVANTAGES:

a. Contributes to continued proliferation of classified information.

b. Increases the scope of the overclassification problem.

c. Will not eliminate difficulties experienced by Departments which do require paragraph marking in incorporating into their system information from documents not paragraph marked.

d. Increases the problems and complexities associated with derivative classification.

e. Makes the enforcement of administrative sanctions for unnecessary and overclassification more difficult.

f. Will tend to impede the declassification process.

OPTION 13:

The new order should mandate the public disclosure of certain specific types of information as are now required to be made public by certain statutes (War Powers Act and others).

ADVANTAGES:

a. May help assure compliance with statues.

b. May contribute to public perception of the Executive Order as consistent with public policy expressed in statutes.

DISADVANTAGES:

a. Might preclude a justified and necessary classification of information which requires protection from disclosure in the interest of national security.

b. Public information policy is not the major purpose of the proposed Executive Order.

c. May contribute to unnecessary classification of information which does not meet the damage criteria of the Order.

OPTION 14:

Continue the provision of the present Executive Order relative to "special departmental arrangements".

ADVANTAGE:

a. Continues present scheme, recognizing special requirements for protection of stated categories of information.

DISADVANTAGES:

a. The minority view is that the present scheme does not adequately recognize the "sensitivity" of the information to be protected.

b. Suggests that individual Departments are authorized to impose special requirements different from those established by other Departments or by national authority.

OPTION 15:

Continue the "special Departmental arrangements" provisions and add a reference to statutes, e.g., 18 USC 798, to serve the purpose of focusing attention on the statutorily recognized sensitivity of information covered by that statute. In addition, add provisions to proscribe automatic declassification of any such information.

ADVANTAGES:

a. Same as Option 14.

b. Provides explicit recognition of the sensitivity of a statutorily specified body of material.

c. Provides for continued protection of sensitive data including that which is already in the public domain.

DISADVANTAGES:

a. May contribute to unnecessary classification of information which does not meet the damage criteria of the order.

b. By Presidential order, would exclude a total body of material from the automatic declassification provisions generally applicable throughout the Executive Branch and to all other information which is classified.

c. Will require the safeguarding and protection of information already in the public domain.

d. May create Congressional and public impression that the total of material covered by 18 USC 798 is never subject to declassification.

OPTION 16:

Retain Section 4(C) of current Executive Order.

ADVANTAGES:

a. Retains present system which is generally well understood by foreign governments and U.S. classifiers.

b. Provides administrative flexibility to Departments.

DISADVANTAGE;

a. May leave ambiguities and uncertainties with respect to the classification of information received in confidence from foreign sources when such information is not classified by those sources and the conditions of receipt are not a matter of record.

OPTION 17:

Provide specific recognition in the new order that information provided to the United States in confidence by foreign governments or foreign sources is classifiable.

ADVANTAGES:

a. Would permit classification of information solely because of the condition of its acquisition even though unauthorized disclosure of it would not damage United States national security.

b. In the view of some, would reduce ambiguities or uncertainties of the treatment of information provided to the United States in confidence from foreign sources.

DISADVANTAGES:

a. Would undermine the thus far recognized basis for classification in the interest of national security.

b. In litigation, would raise the question of the constitutional authority of the President to protect information for reasons other than national defense or foreign relations.

c. Contributes to unnecessary classification.

OPTION 18:

Require use of a unique identifier for foreign government documents and information classified by a foreign government or provided to the U.S. government in confidence by a foreign government or other foreign sources. This would be supplemental to the foreign government classification marking or to the U.S. classification marking assigned, if any.

ADVANTAGES:

a. Identification would enhance foreign government or foreign source confidence in our system for protecting information provided in confidence.

b. In the case of foreign government documents, would provide evidence to a court that material so marked was furnished in confidence.

DISADVANTAGES:

a. May complicate the marking system.

b. May be unnecessary in most cases because a foreign government document would be readily identifiable and should be protected in litigation.

c. Will result in significant cost increases for administering the system.

d. Would prevent use of such information without the disclosure of the source which disclosure, in some cases, would not be desirable and thus, counterproductive from a security standpoint.

OPTION 19:

Modify the definition of the standard for Confidential by including a word such as "appreciable," "significant," or "demonstrable" to modify the word "damage."

ADVANTAGE:

Will tend to reduce the amount of information classified at the Confidential level by effectively clarifying the minimum threshold for classification.

DISADVANTAGE:

Will necessitate the reeducation of original classifiers.

OPTION 20:

Retain the prohibitions against classification now prescribed in Executive Order 11652 and add others.

ADVANTAGES:

a. Demonstrates the interest of the President in assuring that classification authority is not abused.

b. Will give a clear and explicit showing that certain types of information must not be classified and that classification is prohibited for certain purposes.

c. Will engender public confidence in the system.

DISADVANTAGE:

May be found to preclude a necessary classification.

OPTION 21:

Inclusion of a "balancing test" so as to cause the weighing of the relative merits of public disclosure of the information against classification.

ADVANTAGE:

May cause more careful classification decisions and would tend to reduce the amount of information which is classified thereby promoting public accessibility.

DISADVANTAGES:

a. Original classifiers are not necessarily as well qualified to make judgements with respect to possible benefit to the public as they are to the probable damage to national security.

b. In Freedom of Information Act litigations, the courts may demand a showing that the "balancing test" was applied.

RECOMMENDATION:

Consensus was reached in favor of Options 2, 3, 7, 10, 16, 19 and 20. With respect to the remaining Options, there was a divergence of views with no consensus.

ISSUE: Which categories of classified material more than 20 years old could be declassified in bulk under appropriate guidelines.

DISCUSSION: Discussion of this issue will touch on the following points: declassification guidelines - are they needed - who should prepare - what form should they take - how should material classified by or jointly with foreign governments be handled in the guidelines.

E.O. 11652 does not presently prescribe the preparation of the declassification guidelines. At the request of NARS all agencies (which had not previously done so) developed guidelines for the screening of all 30-year-old materials. Over 200 million pages of classified material have been reviewed during the past five years and 99% have been declassified. These guidelines have generally been written in exclusive terms, listing the types of information which could not be declassified. From this experience, it is concluded that: (1) it is impractical to include in the executive order a listing of categories, either inclusive or exclusive, in sufficient detail to guide the actual screening of highly diverse Government records that span time, place and function. Such specification must be left to Departments which have knowledge of the sensitivity of information in their records, the classification authority to act on that information, and an awareness of the security factors affecting the application of that authority; (2) listings of categories excluded from declassification are shorter than such lists of categories to be included in declassification. They are also easier to compile because they include only the most sensitive elements of systems, plans, or operations, and are less likely to maintain classification by oversight.

Over 80% of the permanently valuable 20-year-old classified records created by Federal agencies are still in their custody. The new Executive Order should, therefore, clearly direct the heads of Departments as well as the Archivist of the United States to conduct the systematic review of the permanently valuable records in their custody as they become 20 full years old. Declassification guidelines prepared by Heads of Departments would be shared to facilitate declassification and to ensure prompt opening of all non-sensitive records to the public.

The subgroup also discussed positive steps the government might take to better make available to the public the information being declassified as it becomes available. While more emphasis might be placed on the preparation and publication of agency histories, the government's premier publication of important papers, most of them formerly classified, is in the series Foreign Relations of the United States. Historically the Foreign Relations

Despite the known reluctance of U.S. Departments to assume this responsibility, it is clear that only the subject-matter responsible Departments have the competence to determine whether there is a real need for continued security protection and that the responsible officials of those Departments should be required to exercise their discretionary powers to determine whether the foreign classified record item containing the information or material must be protected for an extended time.

The National Archives feels strongly that this "foreign information" should be treated as our own and declassified on the same basis as our own because of its growing volume, the costs associated with its separation and maintenance in a classified state and the fact that 98% of it does not warrant protection. On the other hand the majority of the subgroup felt that "foreign information" should be excluded from the declsasification provisions of the new Executive Order except where an international agreement on declassification could be reached.

OPTION 1: To direct heads of departments and agencies to develop and make available to their employees and others declassification guidelines for information originated within their jurisdiction; and to also direct the Archivist of the United States together with the heads of Departments to develop guidelines for the systematic declassification of information and material classified by or jointly with foreign governments and international organizations (program to be conducted in consultation with representatives of foreign governments and international organizations with which the U.S. has cooperative security arrangements).

ADVANTAGES:

a. With agency declassification guidelines, Departments would make better and more consistent declassification decisions, thereby reducing classified holdings.

b. Guidelines could be shared with other Departments and lead to more consistent treatment for the same information held by different Departments.

c. Recognizes the dominion of the U.S. Government over its own records and the information in them.

d. Explicitly indicates the U.S. Government's commitment to maximize the release of information to the public.

e. Permits consultation with foreign international organization representatives when the U.S. declassification official determines that it is desirable to attain better understanding without surrendering ultimate authority.

DISADVANTAGES:

a. Preparation of good declassification guidance is expensive and requires the services of highly trained and knowledgeable personnel.

b. May arouse concerns in some countries about information which they provided to the U.S. being released before it is made available to their own citizens.

c. May have some adverse effect on the provision of sensitive information significant to U.S. national interests.

d. If declassification guidance is not carefully drawn, sensitive information will be released.

OPTION 2: To direct heads of Departments and Agencies to develop and make available to their employees and others declassification guidelines for information originated within their jurisdiction; but to exclude from declassification provisions information and material given in confidence which was classified by, or jointly with, foreign governments and international organizations except for such information and material as may be declassified by mutually agreed guidelines developed by the Archivist of the United States, the Heads of the subject-matter interested Departments, and representatives of the cooperating foreign governments of international organizations concerned.

ADVANTAGES:

a. With Agency declassification guidelines, Departments would make better and more consistent declassification decisions, thereby reducing classified holdings.

b. Guidelines could be shared with other Departments and lead to more consistent treatment for the same information held by different Departments.

c. Involves certain allied foreign countries in the process of developing guidelines, thereby avoiding a possible adverse effect on the provision of information important to U.S. national interests.

d. Mutually agreed guidelines will permit U.S. officials to readily declassify the bulk of the older classified materials.

e. Establishes reciprocity in the handling of U.S. information by those countries.

f. Would not "dry up" such free exchange as we now have with foreign governments.

series has led the way in promoting public access. The stated (though unattained) goal for some time has been publication 20 years after the event. To better assure the attainment of that worthwhile goal, the subgroup felt that consideration should be given to including the new Executive Order language which would recognize the merit of the Foreign Relations series.

The treatment of information classified by or jointly with foreign governments is also considered as an appropriate subject for inclusion in the consideration of declassification guidelines. Section 4(C) of E.O. 11652 directs departments to provide appropriate equal protection to information furnished in confidence by a foreign government or international organization. Section 5(B)(1) permits Top Secret classifying authorities to exempt from the General Declassification Schedule "Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it is kept in confidence." But the present Order is not explicit on the matter of handling such non-U.S. originated information when it is 30 years old.

A 1973 Justice Department paper examined the ambiguities of this situation and concluded that present U.S. policy was to exclude non-U.S. originated information from consideration under the systematic review provisions of Section 5(E) of E.O. 11652. That policy was re-examined, however, when the U.S. authorities learned that the British Government was treating foreign documents in their files in the same manner as they were treating British originated information. This policy review was further stimulated by demonstrations that foreign classified information is no more or less sensitive than U.S. originated information concerning the same subjects and that declassification or protection of one could be paralleled by declassification or protection of the other. Finally, it was agreed that the U.S. Government does have dominion over its records and that foreign and international organizations originated information placed into official files become part of the official records of this Government.

In 1976 the State Department's Council on Classification Policy advised the Archivist of the United States to declassify non-U.S. originated information when it is fully 30 years old on the same basis as our own classified information. During the past nine months several million pages of pre-1947 classified foreign documents (exclusive of those held by the Organization of the Joint Chiefs of Staff) have been reviewed against the guidelines developed by the Archivist in consultation with subject-matter interested agencies and have been released. At the present time all foriegn classified information which cannot be declassified under these prescriptive guidelines is being denied to the public by the Archivist of the United States without the benefit of review by more knowledgeable agency specialists.

DISADVANTAGES:

a. Surrenders to some degree the principle of sovereignty of this government over its records.

b. Will require extensive negotiations further delaying declassification of U.S. records.

c. Foreign governments and international organizations may request continued and indefinite protection of some classes of information beyond 30 years which this Government would not find acceptable.

OPTION 3: The new Executive Order should direct heads of Departments and Agencies to develop, use, and maintain current declassification guidelines for information originated by their Departments or within their subject matter jurisdiction. Such guidelines shall specify in reasonable detail what information requires continued protection, and for how long. If the period of continued protection cannot then be determined, the guidelines shall specify a date not more than ten years later for a second review, at which time a date certain for declassification shall be specified. Those Departments and Agencies which hold or expect to receive foreign classified information, shall, with the assistance of the Archivist of the United States as appropriate, advise the foreign governments or international organizations which provided or will provide classified information that such information will be subject to departmental guidelines for declassification or extended protection unless those governments or international organizations consult with the U.S. Department or Agency concerned to develop mutually agreed declassification guidelines for different treatment.

ADVANTAGES:

a. Mandatory declassification guidelines, required to be kept current, would bring about better and more consistent declassification decisions, thereby reducing classified holdings and providing better and more justified protection to those items of continuing sensitivity.

b. The requirement for specificity in guidelines would help eliminate continued classification based on subjective considerations.

c. The option recognizes the government's commitment to maximize the release of information to the pbulic, and should result in matching performance to promise.

d. The provision for specifying either definite dates for declassification or for one further review for the same purpose provides flexibility for dealing with unusual circumstances.

e. Provides for consistency in the treatment of classified information whether of U.S. or foreign origin, absent foreign requests subject to our concurrence for different treatment.

f. Informs cooperating foreign governments of our intent with regard to classified information they share with us, and offers them the opportunity to work out with us different declassification regimes.

g. Maintains foreign confidence that the U.S. will respect their substantive concerns on protection of their classified information.

DISADVANTAGES:

a. Requires reallocation of resources to the preparation and maintenance of declassification guidelines.

b. May complicate declassification reviews and actions if foreign governments insist on treatment different to that which we accord to our own records.

OPTION 4: To avoid any waste of resources by agencies reviewing their records, the new Executive Order should clearly state that only those records constituting the permanently valuable records of the Government (in accordance with 44 U.S.C. 2103) should be reviewed for declassification. Records scheduled for destruction should not be reviewed under this program.

ADVANTAGE:

Will conserve the resources available for application to the declassification review program.

DISADVANTAGE:

None.

OPTION 5: To give appropriate recognition to the merit of the Foreign Relations series in connection with making more information concerning the affairs of the United States Government available to the public, the new Order should include substantially the following language:

All Departments and Agencies will assist the Department of State in its goal to attain a twenty-year publication schedule for the documentary series entitled "Foreign Relations of the United States." The schedule for compiling, editing, reviewing and publishing the Foreign Relations series should not unduly delay declassification of any Agency's foreign relations-related classified information and material.

ADVANTAGE:

Will help assure the attainment of the State Department's goal of publishing at twenty years, thereby increasing the amount of information declassified and published in the public domain.

DISADVANTAGE:

May be inappropriate to single out a particular publication of one particular Department in an Executive Order applicable to the entire Executive Branch.

If Option 1 or 3 above is selected, it is necessary to consider Options 6 and 7 below. If Option 2 above is selected, there is no need to consider Options 6 and 7 below.

OPTION 6: Systematically review for declassification foreign and international organization-originated classified information at the same time as U.S. information is being systematically reviewed.

ADVANTAGES:

a. The most efficient program, and one appreciably less expensive, would be attained through the simultaneous review of all information in the files.

b. Agency declassification specialists would be considering categories of sensitive information for necessary extended protection irrespective of the origins of the information. The less complicated program should therefore be more error free.

c. Only the information determined by the most competent officials to be sensitive and require continued protection would be denied to the public.

DISADVANTAGES:

a. If the program for systematic review accelerates to 20 years we will be opening much more foreign originated information in advance of any allied country.

b. An accelerated opening may have a chilling effect on the provision of information significant to U.S. national interests.

c. Existing liaison arrangements may be further jeopardized if the U.S. Government unilaterally opens information given in confidence on an accelerated basis.

OPTION 7: Irrespective of the U.S. timetable for systematic review, a parallel arrangement for declassification of foreign and international organization originated classified information should take place at the end of 30 full calendar years after origination.

ADVANTAGES:

a. The British and Commonwealth Governments are committed to a 30-year release of records program.

b. The British and Canadian Governments have examined the 30-year declassification guidelines presently being applied in the National Archives and have voiced no strong opposition to its application to their information given in confidence.

DISADVANTAGES:

a. If the U.S. originated classified information is reviewed on an accelerated schedule and all non-U.S. classified information is reviewed on another schedule, about 5% of the classified information in the U.S. records will have to be temporarily withdrawn and 5 to 10 years later 90 to 95% of that material will have to be reviewed again and only then returned to its place in the files. This will be especially costly.

b. Under these circumstances, U.S. reviewing officials would be reviewing records in the same categories perhaps as much as a decade apart in time of origin. Probability of errors and premature release will increase.

RECOMMENDATION: The majority of the sub-group recommended that Option 2, 4 and 5 be adopted. If the new Executive Order directs that information and material classified by or jointly with foreign governments and international organizations be systematically reviewed for declassification, it is the consensus that Option 7 be adopted. A separate issue paper is attached which discusses the authority of the Archivist to declassify certain information; recommend that it be provided to the personnel assigned responsibility for drafting the new Executive Order.

ISSUE:

Whether the Archivist of the United States should exercise authority over information and material which was classified by a former President, his White House staff, special committees or commissions appointed by him, or others acting in his behalf, and whether this authority should extend to information and material not in an archival depository.

DISCUSSION:

Close examination of the interaction of the mandatory review provisions of the present Executive Order and the Freedom of Information Act shows that there is one type of classified document that is not covered by either form of public access request. Several other minor problems with Section 11 that have become obvious since the implementation of E.O. 11652 warrent the attention of the drafters of the new Order. These matters are not addressed here as options, but rather as highly desirable modifications to the language of the new Executive Order.

E.O. 11652 gives authority to the Archivist of the United States to declassify Presidential material, after consultation with agencies having primary subject matter interest, as a solution to a problem that had plagued government officials, historians and archivists for years. An incumbent President faces an obvious political dilemma and risk if he or his staff become directly involved in either opening or closing the papers of his predecessors. The Archivist of the United States, already the custodian of much of this Presidential material through the holding of the Presidential libraries, is far enough removed from partisan politics and the pressures on an agency's classifying officers to consider the needs of national security and at the same time to take account of public and scholarly demands for historical research. The requirement that the Archivist consult with departments having a primary subject matter interest insures the full consideration of relevant national defense and foreign relations questions before determinations are made. The general provisions of Section 11 of E.O. 11652 have worked well and should be retained in a new executive order.

A few minor changes in wording which would solve the minor problems that have become obvious since the implementation of E.O. 11652 center on these points:

a. The limitation of the Archivist's authority to just those materials "in his custody at any archival depository" should be dropped so that someone will have the authority to declassify information and material classified by the White House found among agency records, private papers, and other collections, etc. At present, no one has the authority to declassify such material;

Attachment

b. The Archivist's authority should be limited to materials classified by a former President, since an incumbent President will obviously declassify his own records;

c. Reference to the "terms of the donor's deed of gift" should be deleted because it is not pertinent to security classification and reflects a statutory responsibility of the Archivist entirely apart from national security requirements; and,

d. Add the word "downgrade" to the Archivist's authority so that he has the authority not only to review and declassify, but also explicit authority to downgrade classified documents and records.

RECOMMENDED LANGUAGE IN A NEW EXECUTIVE ORDER:

After the termination of a Presidential administration, the Archivist of the United States shall have authority to review, downgrade and declassify information and material which was classified by the President, his White House staff, special committees or commissions appointed by him, or others acting in his behalf when this information or material is not part of the records of an agency subject to Federal records statutes. This authority shall be exercised only after consultation with the Department having a primary subject matter interest.

ISSUE : How to promote increased public access to information no longer needing classification through a more rapid and systematic declassification program

DISCUSSION :

The subject of achieving more rapid declassification of information is one difficult to discuss as something apart from the subject matter of other subgroups. This results from the fact that achieving more rapid declassification is an issue central to the overall Executive order revision project, the goals of which are to insure that only items requiring classification are classified to begin with and to effect declassification of information as soon as it is possible to do so, all in the interest of achieving greater openness in government. Nonetheless, there are a number of proposed changes from the current Executive order on classification that fall squarely upon the point of achieving more rapid declassification.

The suggestion has been put forth that consideration of the time period for which a document remains classified should be divorced from consideration of the appropriate level of classification. What is proposed is that a date be set for declassification of a document based on the best estimate of the classifier as to when it may be declassified. The period of classification would not be tied to level of classification, as is now done under the General Declassification Schedule with Confidential, Secret and Top Secret classification actions resulting in classification being maintained for periods of six, eight and ten years, respectively. Under the proposed system, there would be a maximum period which could be embraced by the classifier's estimated declassification date. The consensus was that such period would be six years. Continuation of classification in excess of the prescribed norm, say, for example, nine years or any other specified period of years not in excess of twenty could only be done by an official specifically designated to exercise original Top Secret classification authority. The official authorizing such continuation of classification should be required to make a record of his action, including his identification and reason for his decision. This last point would parallel to some degree the current authorization of Top Secret classifiers to exempt from the General Declassification Schedule information within four stated categories.

Another approach to achieving more rapid declassification, which may be considered additional to other more specific measures, is that of building in a presumption against classification in certain decision making processes. The presumption would be rebuttable, of course, but might be operable

whenever the classified status of a document was challenged or after a set period as outlined in the previous paragraph. The presumption against classification would eliminate instances of classification being continued merely because a speculative argument could be made for maintaining classification. Under the presumption against classification, a set period of classification would be extended only when the relevant factors and circumstances at the time of review were found to be those which warrant original classification. As a companion of the presumption against classification, measures would be taken to minimize the threat of adverse repercussions to an individual employee should he in good faith make an erroneous declassication in exercising his declassification authority. Declassification authority would also be decentralized to the lowest possible level. There may be a need for institutionalizing a system for intra-agency challenges to classification. The vehicle for building in the presumption against classification would be the overall thrust of the Executive order coupled with a firm and explicit statement of policy in the preamble. Specific criteria for declassification would be included in the Executive order. However, with the thrust in the direction of declassification and certain protections for errors in judgment being accorded the declassifier, certain problems can be perceived regarding differentiating between good faith and bad faith declassification actions by lower level employees.

It is believed that the effective promotion of public access to official records through declassification must be given as much attention as the denial of public access through classification. With few exceptions, there are simply not enough agency resources devoted to declassification efforts. Declassification reviews that are provided for under the existing Executive order are rarely being accomplished as they should. It is proposed that any new Executive order in this area direct heads of agencies to devote sufficient resources to carry out the declassification program provided for by the order.

A point stirring considerable debate was that of granting access to classified information to certain individuals not acting in an official capacity and not holding the clearance normally required. Typical of individuals granted such access under the current Executive order are former Presidential appointees and historical researchers. (On a related point, there apparently is a serious problem involving the interposition of interagency barriers between official historical researchers, who themselves act as a catalyst for declassification, and the materials they need. It is recommended that this problem be handled in the form of government-wide interagency agreement.) In considering the granting of access to nonofficial researchers, the consensus was that it is difficult to discern a persuasive basis on which to award privileged access to certain individuals and not to the general public. The danger is not granting a special access is that for years only "official histories" will be available of important incidents in our national experience. Whether granting access to selected individuals under controlled circumstances solves the "official history" problem is unclear. In any event, a majority seems to feel that Section 12 of the current Executive order is of so little utility for promoting increased

general public access to official information that it would not be advisable to include it, for that purpose, in a superseding order which would instead make the fruits of an accelerated declassification program available to all persons at the same time. However, the contrary view is also held. But there is the view that the public benefits from the more rapid declassification spurred by the special access provisions and that to delete section 12 as it relates to unofficial access would appear to the historical community to be a retrogressive step.

Section 5(E) of the present Executive order requires the declassification of classified information and material after thirty years except for such specifically identified information and material which the head of the originating department personally determines in writing at that time to require continued protection in the interest of national security. Advancing the thirty-year time frame for automatic declassification to twenty-five or twenty years would be perceived as a significant step in promoting increased public access to information and material no longer requiring protection. There was a consensus that the twenty-year frame is realistic and ought to be adopted even though a large proportion of the documents of certain agencies would still have to remain classified after twenty years. However, it was noted that such a change would have a severe impact on available resources allocated to the task of performing systematic reviews of classified information and material, both in the National archives and the several departments. The recommended change from thirty to twenty years would create an immediate ten-year backlog of material requiring review for declassification. The national Archives is steadily falling behind in its effort to maintain the thirty-year line mandated by the 1972 order. Thus, NARS points to the need to provide for a gradual phase-in over a ten-year period, for example, of a policy requiring twenty-year systematic review of information and material classified under E.O. 11652 and previous orders coupled with an increase of resources. If such resources were not forthcoming through the budgetary and appropriations process, sensitive information within the ten-year backlog could not be identified for continued protection through screening, and might be subject to forced disclosure under the Freedom of Information Act. It is relevant to note that additional resources to handle the burden of processing FOIA requests have not been provided, even though the Congress in passing that Act acknowledged the possible adverse resource impact and invited departments to request resources if they could prove the need. Additional considerations in this general area are discussed in an appendix hereto which reflects the views of the NARS representative to the Sub-Group.

Under the present order there is a perceived retarding effect on the declassification process deriving from the provision of four stated exemption categories which seem to induce classification of the information encompassed therein and continuation of that classification beyond the period

prescribed by the General Declassification Schedule. Elimination of the broad exemption categories is the solution proposed to remedy this. Extension of classification would only take place in accordance with carefully defined criteria and as deemed necessary by those possessing Top Secret classification authority. It was the consensus that heads of departments should have authority to extend the classification lifespan of their information and material beyond the proposed twenty-year limit at any time during the classified lifespan of the information, rather than at the time of automatic declassification as is presently required. Further, there is agreement that heads of departments should be able to either specify a fixed period of continued protection or specify a date for further review. Their discretion in this area would be monitored by the oversight apparatus to be established under a new order.

During the discussion it became evident that information generated by certain agencies, notably NSA, CIA, and OJCS, in large measure do not lend themselves to rapid declassification because their sensitivity is geared to technological or foreign relations considerations, or reveal intelligence sources and methods or currently sensitive operational planning formation. However, this fact should not impede efforts to declassify information not falling in these categories.

Options considered, some of which offer the potential for more rapid declassification and hence for increased public access to official information, include the following:

OPTION 1: Maintain the provisions of the current Executive order regarding declassification.

ADVANTAGES:

- Requires no increase in resources.
- Preserves a policy that has domestic and foreign circulation and acquiescence.
- Review at 30 years has had a high release rate (over 98%).
- There will be a minimum likelihood of error as guidelines already promulgated have been tested in the review of millions of records with no known release of sensitive national security information.
- Release by foreign and international organizations of their classified information frequently occurs simultaneously.

DISADVANTAGE:

- Does not meet the mandates implicit in PRM/NSC-29, i.e., simplification of the system, public accessibility, earlier bulk declassification, etc.

OPTION 2: Establish a new declassification system which, in substance, would: (1) divorce the time period of classification from the level of classification; (2) require an original classifier, within the limits specified in the authority delegated to him, to fix the shortest period of classification which he determines to be warrented; (3) limit the authority of original Confidential and Secret classifiers to continue classification to a period of six years; (4) limit the authority of original Top Secret classifiers to continue classification beyond six years but not in excess of twenty years; (5) prescribe that only a Department head may continue classification beyond twenty years; (6) provide that, unless declassified earlier or extended beyond twenty years by the head of a Department, information classified pursuant to this Order shall be automatically declassified after twenty years; (7) require that authorities who extend classification beyond six years record their identity and reason for their decision; and, (8) require that with respect to each original classification, a date would be fixed for automatic declassification or for review to determine the need for continuation of classification.

ADVANTAGES:

- A shorter norm for continuation of classification would be established.

- Higher level of classification would not be assigned in order to achieve a longer period of classification protection.

- Responsibility for continuation of classification beyond normal time periods would be fixed.

- A greater volume of classified information would become available for release to the public after a shorter period of classification.

DISADVANTAGES:

- The new approach would necessitate revision of departmental implementing regulations and retraining of original classifiers.

- With automatic declassification taking place after shorter periods, there may be an increased problem in terms of notifying distributees of changes in classification period, due to changed circumstances, or perceptions, than is now the case under the General Declassification Schedule.

OPTION 3: With respect to information and material classified under previous Orders, the new Order would provide that: (1) if the material is already marked for declassification within twenty years of date of origin, it shall be declassified accordingly; and (2) if not so marked, shall be declassified in accordance with declassification guidelines promulgated by heads of Departments as prescribed by the new Order.

ADVANTAGES:

- Accelerate public availability of information on prior government activities and policies.
- Meets the mandate implicit in PRM/NSC-29.
- Will lead to better and more consistent declassification decisions, thereby reducing classified holdings.

DISADVANTAGES:

- Will create an immediate review backlog.
- Will require considerably more resources to fully attain the twenty-year objective.
- May increase the risk of premature disclosure of classified information.
- Preparation of good declassification guidance is expensive and requires the services of highly trained and knowledgeable personnel.

OPTION 4: Build a presumption against classification and for declassification into the scheme of a new Executive order.

ADVANTAGE:

- The balance would be tipped in favor of more liberal declassification decisions.

DISADVANTAGE:

- May prove difficult to fine tune declassification policies at lower echelons.

OPTION 5: Have a mandatory declassification review system within an agency providing a mechanism for internal challenges to classification. Under such a system, whenever a classification action was challenged and declassification was refused, either by the original classifier or by one possessing declassification authority, there would be an automatic referral to an agency review committee which would decide the matter.

ADVANTAGES:

- A more effective interim review program would result.
- Encouragement to initiate declassification actions would be given to those best positioned to identify information that could be declassified.

DISADVANTAGE:

- This option holds the potential for placing an additional burden on agency resources to an extent not easily estimated in advance.

OPTION 6: Eliminate present system of preferential access to classified material by nonofficial researchers.

ADVANTAGES:

- Would save cost of personnel security checks and other administrative costs associated with insuring the trustworthiness of these personnel and servicing their needs.

- Would reduce the risks of unauthorized disclosures.

- Would eliminate an objectionable preference afforded to comparatively few.

DISADVANTAGES:

- Could be interpreted as retrogressive by the historical community.

- May increase the number of requests for declassification under FOIA and mandatory review provisions of the Order.

- Would probably decrease the speed with which unofficial historians publish accounts of certain aspects of national defense and foreign relations.

OPTION 7: Authorize the granting of access to classified material to persons outside the Executive Branch who are engaged in research, provided the head of the originating Department:

(1) Determines in writing that access is consistent with the interests of national security;

(2) Takes reasonable actions to insure that the information is not subject to unauthorized disclosure; and,

(3) Takes reasonable actions to ensure that access is limited to specific categories of information over which that Department has classification jurisdiction.

ADVANTAGES:

- Would continue a policy which is indicative of openness in government.
- Would facilitate the early publication of historical material in a form readily available to the public.
- Eliminates preferential treatment for former officials.

DISADVANTAGES:

- May subject classified information to unauthorized disclosure.
- Incurs expense of personnel security checks and other administrative costs involved in determining trustworthiness and review of notes and manuscripts.

OPTION 8: Include in the new Order a requirement that heads of Departments designate officials at the lowest practicable echelon of command and supervision to exercise declassification authority with respect to classified material in their functional areas of responsibility.

ADVANTAGES:

- Facilitates resolution of classification conflicts.
- Facilitates declassification and release review.
- Demonstrates increased emphasis on declassification.
- Places declassification responsibility on those best qualified to make those determinations.

DISADVANTAGES:

- Without full coordination, it may result in conflicting declassification decisions.
- Declassification of information in a functional area may make classification in a related functional area impractical.

OPTION 9: Include in the new order a requirement that heads of Departments budget for and provide adequate resources to carry out full and effective implementation of the Order.

ADVANTAGES:

- Demonstrates Presidential concern.

- Will cause top management support.

- Will assure effective implementation.

DISADVANTAGE:

- May reduce the options of heads of Departments in establishing resource priorities.

OPTION 10: Include in the new Order a section providing declassification criteria.

ADVANTAGES:

- Would fix common guidance for use throughout the Executive Branch.

- Would be viewed by the public as progressive and indicative of Presidential intent to avoid the continuation of classification beyond its useful life.

- May result in earlier and more uniform declassification.

DISADVANTAGES:

- Might result in declassification of information and material which under particular circumstances could be premature.

- May be difficult to develop criteria which are all-inclusive.

RECOMMENDATION: It was the consensus of the Sub-Group that Options 2, 3, 4, 8, 9 and 10 be adopted. With respect to the remaining options there was a divergence of views.

CONSIDERATIONS ON ADVANCING THE AUTOMATIC DECLASSIFICATION DATE TO 20 YEARS FROM DATE OF ORIGIN

Section 5(E) of E.O. 11652 directs that all information and material classified before June 1972 shall be systematically reviewed for declassification by the Archivist of the United States by the end of the thirtieth full calendar year following the year in which it was originated. When the program for systematic review was inaugurated in the National Archives in October 1972 (following approval of the FY 73 budget request and after denial by Congress of a supplemental budget request for FY 72), there were about 60 million pages of permanently valuable classified records in the National Archives of the United States which were already 30 years old. In the 4½ years the program has been operating the especially hired and trained declassification review staff of the National Archives, together with declassification specialists from the agencies, have reviewed and declassified approximately 200 million pages of documents predating 1947. Less than one-half of one percent have been determined to require continued security protection. This low exclusion rate reflects the fact that the greater part of these records related to World War II, which facilitated declassification. Experience in the systematic review of documents from the 1946-50 early cold war period indicates that nearly 80% of them must be carefully screened, page-by-page, to determine whether they contain sensitive information. Thus, many more hours are required to review the same amount of more-recent records. Further, approximately 2% of the records in this time frame require extended protection. With the resources available to the National Archives' systematic review program for thirty-year-old records ($1.4 million per year) it has taken nearly five years to complete the review of the original WW II classified records backlog, and the program is now steadily falling behind in its effort to maintain the thirty-year line mandated in the 1972 Order. While much of the review effort has been devoted to the permanently valuable records in the custody of the National Archives and the Franklin D. Roosevelt Presidential Library; additional programs have been carried on by declassification specialists in the Department of Defense, CIA, and ERDA on 30-year-old records in agency possession.

Before dismissing the present scheme out of hand it might be well to examine the apparent advantages of retaining the review point at 30 full years:

a. To obtain and maintain the 30-year line will require little increase in resources. An exception to this is the FBI which has not yet inaugurated a systemated review program for its older records;

b. It would preserve a policy that has domestic and foreign circulation and acquiesence;

c. The review at 30 years has had a high release rate (over 98%);

d. There will be a minimum likelihood of error as guidelines already promulgated have been tested in the review of millions of records with no known release of sensitive national security information; and

e. Release by some major allied foreign Governments of their classified information occurs simultaneously.

While these are undeniably attractive points, a 30-year systematic review schedule does not meet the mandate implicit in PRM/NSC-29 to advance the scheduled review to a 20-year line.

The clear advantages of advancing the systematic review to the line of 20 full years are:

a. That it would accelerate the public availability of information on prior Government activities and policies; and

b. Probably about 90% of the permanently valuable records to be reviewed can be released when the fullcycle of review is completed.

These advantages can only be obtained at a price--a monetary expense of sizable proportion and a potential risk of premature release of still-sensitive information (especially significant in the early release of intelligence records) as the whole Government rushes to catch-up without tested declassification guidelines nor personnel experienced in identifying the increasingly sensitive more recent records.

The monetary price of advancing to a 20-year line can be expressed in terms of anticipated level of effort over the present level of effort. The best figures for agency allocations exclusively devoted to the systematic review of 30-year-old records is about $4 million per year. In our judgment it will require nearly five times the present amount of effort in manpower alone to catch-up to the 20-year line <u>if</u> agencies are given 10 years to attain that objective. The total cost over the 10 years needed to accelerate the date of release would amount to about $200 million.

The factor of five is based on the following considerations:

a. Development of adequate 20-year declassification guidelines will require the best efforts of numerous top professionals and highly skilled technicians.

b. Training of the hundreds of personnel hired or reassigned to declassification screening and reviewing duties will also require the time and effort of these same high-priced and busy staff members.

c. The costs associated with: (a) hiring new personnel and obtaining their security clearances, (b) acquiring and preparing additional work space to accommodate them, and (c) time expended in training and supervising the work-force will add several millions of dollars to the total price of the program.

d. If 90% of the records over 20 years old and 98% of the records over 30 years old can be declassified, it follows that from 2% of the oldest records to 10% of the more recently dated records will have to be identified, reviewed by an agency specialist knowledgeable in that category of potentially sensitive information, withdrawn from the files and provided extended security protection pending automatic declassification or re-review.

e. Until new agreements are reached, all foreign and international organization-originated classified information less than 30 full years old may have to be withdrawn.

The conclusion reached was that the 20-year option is highly desirable and would be readily attainable if the categories of intelligence sources and methods* and foreign and international organization-originated classified information could be excluded from the requirement to attain and maintain the 20-year automatic review schedule. The National Archives representative did not feel that any special exceptions to the Government's entire declassification program should be made for these two general categories of information which in his experience are pervasive in the Government's records. Aside from this intelligence community concern, the key question here is the willingness and ability of executive and legislative budget authorities to provide the affected agencies with resources proportional to the objective. A decision on the resource commitment will determine the attainable objective. The 30-year goal, which is not now being met, must prevail if no additional resources are provided. The 20-year goal, while highly desirable for reasons of policy and philosophy, requires a significant and sustained commitment of resources which other public priorities may not permit.

* For the purposes of the new Executive Order, intelligence sources and methods may be defined as follows: A source is a person, organization, or technical means which provides intelligence, subject to protection of identity and intelligence relationship, and is vulnerable to counter action and thus could be lost or diminished in effectiveness should identity become compromised. Methods are the means by which support is provided to, or intelligence received from, sources when such means are vulnerable to counter action or compromise essential privacy if they are compromised.

ISSUE: Overlaps between the new Executive Order and the Freedom of Information Act as amended and the Privacy Act.

DISCUSSION: The Sub Group concentrated on several matters within this issue which require attention to ensure that achieving increased compatibility between the new Executive Order and the amended Freedom of Information Act (FOIA) does not unduly expose current Presidential papers to intrusive requests nor deny the present methods of access to the papers of a former President.

Section 5(C) of E.O. 11652 provides the public (and Departments as well) with a means for demanding the review of all classified information and material more than 10 years old. The requester need only "describe the record with sufficient particularity to enable the Department to identify it" so that "The record can be obtained with only a reasonable amount of effort." The amended Freedom of Information Act (FOIA) provides persons with the right to request classified information and material which is part of an official record of the Government as defined in 44 USC 3301 without regard to the age of the records. To a large degree, the mandatory review provision and FOIA overlap in their application. There are, however, several important exceptions:

a. Only the mandatory review provision of the present Order applies to non-Federal records or donated historical materials (such as the papers of former Presidents and other officials in Presidential libraries and classified documents in non-Federal repositories such as university collections);

b. The mandatory review provision only applies to classified documents which are at least 10 years old while the FOIA applies to all Federal records regardless of their age but does not apply to classified documents which are not "Federal records."

c. The mandatory review provisions of the Order require that requesters identify a record with "sufficient particularity," imposing a test stricter than the one required by the FOIA;

d. The FOIA specifically includes language requiring release of the segregable portions of a document which under the Act cannot be exempt from release. The mandatory review provisions of the Order do not;

e. The FOIA imposes a 10-day deadline for initial response while the NSC directive which implements the present Order makes mandatory review requests subject to a 60-day deadline for initial response;

f. The appeal routes are separate, with FOIA requests appealed to Department heads and then to the courts while mandatory review requests are appealed to Departmental committees and then to the ICRC.

Discarding the mandatory review provision would be a retrogressive step because it would allow no route for requesters to require classification review of non-Federal records (such as those in a Presidential library). For example, in calendar year 1977, approximately 100,000 pages of historically important classified documents from the Truman, Eisenhower, Kennedy, and Johnson Presidential Libraries will be submitted to agencies for classification review under the mandatory review provision of E.O. 11652. Good and sufficient reason dictates that the mandatory review provisions of E.O. 11652 be carried forward into the new Executive Order.

Most of the criticism directed at the mandatory review provision has focused on the differences between the Executive Order and the FOIA. The options on this issue center around reducing the discrepancies between Executive Order 11652 and the Freedom of Information Act. These differences are addressed in Options 1-4, below.

OPTION 1:

Drop the limitation imposed by the present Order under which only classified information and material at least 10 years old may be requested for mandatory review.

ADVANTAGES:

a. Because agency records less than 10 years old are already subject to review for release under the FOIA, dropping this 10-year provision would primarily provide a means for requesting access to an incumbent President's

papers and those documents of a former President that are very recent in origin, none of which are subject to the FOIA.

b. Brings the requirements of the E.O. and the FOIA more in line with each other.

c. Results in more openness in Government and more access to high-level contemporary papers which are not subject to the FOIA.

d. Reduces expensive storage requirements by reducing the number of classified documents in Presidential papers.

DISADVANTAGES:

a. Creates an anomalous situation in which requesters have a method for demanding classified but not unclassified documents from a President's papers.

b. Would make more classified information and material subject to an extremely expensive classification review system, yielding small results at high cost. Generally, there is very little point in spending the time and money to review very recent and very high-level classified information because of the high rate of continued classification of any substantive documents.

c. Creates an impracticable system in which a former President's papers would be subject to public demand for review of specific items while in transit from the White House to a permanent Presidential Library or in temporary warehouse storage before elementary boxing and processing by archivists could be completed.

d. Would require a large staff increase within the Executive Office of the President and the Presidential Library system of the National Archives and Records Service.

OPTION 2:

Drop the 10-year prerequisite for mandatory review of Federal records (as defined in 44 USC 3301) but not for Presidential materials, donated historical materials as defined in 44 USC 2101, or other non-Federal records.

ADVANTAGES:

a. Brings E.O. requirements more in line with FOIA without increasing cost, since Federal records less than 10 years old are already subject to review under FOIA.

b. Would be compatible with the recommendation of the National Study Commission on Records and Documents of Federal Officials that access to a President's public papers should be subject to restrictions imposed by the President for a period not to exceed fifteen years, after which there would be general public access, subject only to such restrictions as are necessary in the interest of national security or to protect against a clearly unwarranted invasion of privacy. To drop the 10-year provision in its application to a President's public papers in the new Executive Order would seriously impact on the Commission's recommendations to Congress.

c. Gives the appearance of more openness.

DISADVANTAGES:

a. May generate increased workload with respect to Federal records less than 10 years old.

b. Would establish a necessity for Departments to provide redundant review systems with respect to Federal Records less than 10 years old.

OPTION 3:

Amend the present phrasing of the mandatory review provision as it is expressed in E.O. 11652 so as to direct Departments to declassify any reasonably segregable portion of a record or donated historical document after deletion of information which must remain classified.

ADVANTAGES:

a. Brings E.O. more in line with FOIA requirements.

b. Would bring uniformity of procedure since sanitizing (release of segregable portions) is already being done in several major agencies.

c. Would result in the release of more official information to the public.

DISADVANTAGES:

Sanitizing of documents requires staff time to identify and segregate information. A considerable increase in costs would be sustained by several agencies.

OPTION 4:

Revise the mandatory review provision of the present Order so as to require the same time deadlines as the FOIA.

ADVANTAGES:

a. Reduces confusion by bringing E.O. response-time requirements in line with the FOIA requirements.

b. Would result in more rapid treatment of mandatory review requests.

DISADVANTAGES:

a. The 10-day deadline for FOIA requests is not practicable now for a large number of requests and would be totally impracticable for documents containing national security information that must be cleared with several agencies or for documents that must be mailed from distant Presidential Libraries for review in Washington, D.C.

b. Would increase the expense and the staff time devoted to the mandatory review process authorized by the Order.

c. Would require major overhaul of a program that is already responsive to the public and not a source of widespread complaint.

RECOMMENDATION:

That a mandatory review provision be retained in the new Executive Order and that the provision include: a 10-year exemption for documents that are not Federal records (Option 2); that segregable portions of a document be declassified when the entire document cannot be declassified and the release of the document is not prohibited by any other statutory or departmental requirements (Option 3). In addition, the new Executive Order not change the present response deadlines prescribed under the Order.