REPORT FOR: Members of the Working Group on Implementation and Review, PRM/NSC-29 Ad Hoc Committee

FROM: Sub-Group I/R-2

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

---

This Issue-Option-Recommendation paper is submitted to the Work Group Chairman on Implementation and Review, acting under the direction of the Ad Hoc Committee pursuant to PRM/NSC-29.

The paper addresses the relative problems of misuse of the classification system and the unauthorized disclosure of classified information by government officials. It sets forth various options and several recommendations to arrest these problems. Specifically, the Sub-Group was asked to consider the issue of "what kinds of disciplinary actions can be taken to prevent the misuse of the security classification system by government officials." Arising from this issue are three sub-issues which are set out below in discussing the various options and recommendations. The Sub-Group has found it more convenient to use the sub-issues in

discussing our options and recommendations as called for in the Format. Of course, in discussing these sub-issues we address the parent issue.

The Sub-Group concludes that the present sanction in E.O. 11652 is too narrow, in terms of available sanctions, and is not adequate to deal with the two problems stated at the outset. It urges the Ad Hoc Committee to recommend that the new Executive Order set forth sanctions, as recommended herein, which will provide more effective methods to prevent the misuse of the classification system and the unauthorized disclosure of classified information. The Sub-Group considered such preventive methods as disciplinary measures, civil fines, criminal sanctions, increased use of polygraph tests and secrecy agreements.

In the main, DOD, CIA and State are in agreement on all recommendations contained in this paper, while DOJ dissents from the recommendation that the Special Coordination Committee consider further review of alternative proposals for civil or criminal sanctions for unauthorized disclosure of classification information to determine if legislation is desirable. DOJ's position on this recommendation is that "the price for passage of legislation generally criminalizing the unauthorized disclosure

of classified information is a price too high to pay for the marginal utility of such legislation." DOJ also dissents from the recommendation that the use of uniform secrecy agreements be instituted Government-wide. Since the representatives of the White House and NSC did not participate in the Sub-Group's meetings the recommendations set forth below may not necessarily reflect their views.

ISSUE: Is the sanction in E.O. 11652 ("repeated abuse . . . shall be grounds for administrative reprimand") stiff enough? Should there be criminal sanctions for extreme misuses, such as use of classification to cover up criminal activities or gross mismanagement?

DISCUSSION: E.O. 11652 expressly prohibits classification in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or 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." These prohibitions are sound policy and should be included in any superseding Order. Additional prohibitions are being considered in Sub-Group CD/1. Enforcement of these prohibitions

is essential to the integrity of the classification system itself and to public confidence without which a classification system will fail.

OPTION I: Retain the provisions of Section 13 of E.O. 11652 and of Section X.D. of the NSC Directive of May 17, 1972.

ADVANTAGES: Departments could continue present practices and systems for enforcement of compliance with the operable provisions of the classification system.

DISADVANTAGES: The disadvantage of this Option is that it only allows for a single sanction, and fails to provide for a range of sanctions. However, the present administrative actions allowed are not sufficient. The sole administrative sanction prescribed by Section 13 of E.O. 11652 for wrongful classification 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.

The Sub-Group as a whole feel that administrative sanctions as set forth in Options 2 and 3 will prove to be adequate to achieve the necessary compliance throughout the Executive Branch.

There does not appear to be necessity for specific criminal sanctions for violation of the prohibitions. In the extreme case that an obstruction of justice is caused by a classification made for the prohibited purpose, the criminal sanction which attaches to that offense could be invoked.

OPTION II: The Order should include a section concerning enforcement which will provide for administrative sanction for willful origination or continuation of classification of information in violation of the Order or an implementing directive; releasing or disclosing or causing release or disclosure of classified information or material in a manner not authorized by the Order or an implementing directive; or other violations of the Order.

ADVANTAGES: The importance of strict compliance with Executive Order standards and criteria for classification and declassification would be properly emphasized. A practical result of strict compliance with those standards and criteria will be a smaller quantity of classified information, earlier declassification of that information and more and earlier public availability of information concerning the affairs of Government.

The importance of strict compliance with Executive Order policy with respect to protection of classified information and material from unauthorized disclosure would be properly emphasized.

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

A clearly enunciated and well administered program of enforcement based on administrative sanctions will be a more effective deterrent to non-compliance than is the risk of effective prosecution for violation of present criminal statutes.

Responsibility for enforcement of compliance 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.

Heads of Departments will specify the provisions of the Order and implementing directives violation of which 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 Department.

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

OPTION III: The Order should include a section concerning enforcement which will provide for a range of sanctions, e.g., warning, reprimand, suspension without pay, removal, which may be imposed for Option I abuses or violations in accordance with applicable law and Departmental regulations.

RECOMMENDATION: The new Executive Order should include sections which incorporate the categories set forth in Options II and the range of sanctions set forth in Option III. The Executive Order should also direct that violation of relevant criminal statutes, e.g. 18 U.S.C. 793, 794 and 798, be referred promptly to the Department of Justice for investigation and for prosecution as appropriate.

ISSUE: Should the Ad Hoc Committee consider the issue of what sanctions (civil or criminal) should be adopted, modified, or continued, for the unauthorized disclosure of classified information?

DISCUSSION: The members of Sub-Group I/R-2, Working Group on Implementation and Review, have read with interest the draft subcommittee Report to the SCC, dated 1 June 1977, on "Unauthorized Disclosure of Sensitive Information." That report concludes that a thorough review of the classification system is a necessary first step to any resolution of the problem of unauthorized disclosures, and we believe that the efforts to revise the existing classification system can do much to support executive branch attempts to safeguard information. The greater is the integrity of the system, the greater will be the support to uphold it. However, the sub-group members are not persuaded by the draft report to the extent it recommends not to seek legislation to impose sanctions for the unauthorized disclosure of classified information. On the contrary, we believe the dissenting comments appended to the report have placed upon that recommendation sufficient doubt as to warrant that further attention be given, not only to whether any sanctions should be authorized, but to developing feasible alternatives. The dissents appear to focus more accurately than the draft report on what we perceive to be the crucial issues involved; therefore, we believe that the question of criminal and civil sanctions deserves more consideration than the subcommittee has given.

Our concern in this regard arises because we believe that some sanctions are desirable for unauthorized disclosures, and we are persuaded by the dissent that the problem of prosecuting those responsible for unauthorized leaks may not necessarily result only from an unwillingness to pay the price of enforcing existing statutes. Rather, we agree that existing statutes are generally not applicable to all unauthorized disclosures, such as anonymous leaks to the press, and that further legislation is needed. The PRM/NSC-11 subcommittee itself states:

> Because inadequate coverage of existing laws and the difficulties involved in prosecutions under them, the Executive Branch has attempted without success since at least 1957 to obtain new legislation which would generally criminalize the unauthorized disclosure of classified information. At page 9.

Nevertheless, the subcommittee drafters conclude that for a variety of reasons no new legislation should be sought.

One of the major reasons for this conclusion was that intelligence agencies have often refused, prior to any investigation of a leak, to declassify information determined to be essential for purposes of prosecution. This difficulty seems to be capable of resolution, and we believe that the dissenting position raises some valid points in this regard. We are

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 of this and related information, 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 whether or not it is actually appropriate to declassify such information or reveal intelligence sources and methods. Thus, while we are sympathetic to concerns that investigations are fruitless if conducted without a firm commitment to prosecute, we are 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, however, often may preclude consideration of factors necessary to an informed decision of whether or not to declassify. We urge further review of this problem.

Regardless of such policy, however, there are a number of alternatives which this sub-group believes should be explored by the Special Coordination Committee. Since the PRM/NSC-11

subcommittee failed to discuss proposals for legislation which it is our understanding had considerable support, we urge a complete review of those alternatives. There may very well be various conclusive political and security costs involved in investigating and prosecuting leaks, and price for passage of legislation generally criminalizing the unauthorized disclosure of classified information may be too high a price to pay for such legislation; however, the Subcommitree Report to the SCC has not persuasively presented its position. The dissenting comments point out with considerable force the failure of the draft report to adequately describe the range of viable options.

RECOMMENDATION: We recommend to the Special Coordination Committee that it undertake a review of alternative proposals for civil or criminal sanctions for the unauthorized disclosure of classified information, since it has been the position within the executive branch that some legislation in this regard is consistently desirable. If the SCC determines that departure from the status quo is not feasible at the present time, at least it shall have done so after full consideration of the alternatives. We simply urge further consideration of every alternative and careful weighing of all factors. DOJ dissents.

ISSUE: Should the new Executive Order require that each person who has access to classified information execute a secrecy agreement as a condition of being granted access?

DISCUSSION: The desirability and effectiveness of using secrecy agreements as a means to prevent disclosure of classified information was discussed in some detail in the Subcommitee Report to the SCC, dated 1 June 1977, pursuant to PRM/NSC-11. In E.O. 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. At present most departments and agencies have executed agreements to comply with E.O. 11905, but there is some question as to whether they are in full compliance. The exception is the CIA which already had a secrecy agreement program applicable to all employees. Under the CIA's program an employee is required to execute a secrecy agreement as a condition of employment, and other persons execute such agreements as a condition of gaining access to classified information.

CIA would not like to see the new Executive Order contain any provision which would require its present employees to reexecute a secrecy agreement. State and DOD prefer a

Government-wide uniform secrecy agreement as a condition of obtaining access to classified information. This issue of whether any secrecy agreement program mandated should be retrospective or prospective. The Sub-Group agreed as a whole that this issue should be left to the Ad Hoc Committee.

DOJ is not opposed to secrecy agreements in principle. However, it raises questions about their utility as a preventive tool. DOJ feels that the beneficial returns from the use of secrecy agreements are probably for less than the administrative burdens and costs.

DOJ agrees that secrecy agreements may, in some instances, serve as an additional deterrent and may, in some instances, provide the Government with the legal vehicle of a civil injunction, but agree that it will not deter those who are predisposed to disclosure and will probably be demeaning and insulting to those who are not. Its usefulness in seeking an injunction, says DOJ, 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 agrees 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, it 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. DOJ believes that the President has the power to impose such a requirement upon the military as Commander-in-Chief of the armed service, and upon career civil service entrants and present government employees under 5 U.S.C. §§3301 and 3302.

DOD raises the question that since a secrecy agreement is a contract where is the necessary consideration when the secrecy agreement is based upon obtaining access to classified information. DOJ and CIA believe that the Government's consideration is the employee's promise to safeguard classified information and to refrain from disclosing the same, and that the employees' consideration is the ascertaining of a job that requires access to classified information, which he otherwise could not hold.

It was also suggested that a provision be included calling for liquidated damages or a civil fine. DOJ objects 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.

OPTION IV: 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.

ADVANTAGES: This Option will have educational value and will serve as a deterrent, and it will also allow the Government to seek a civil injunction to prevent the disclosure of classified information.

DISADVANTAGES: First, the administering of any secrecy agreement program may out weigh its benefits. Second, the Government's ability to seek an injunction to prevent disclosure would probably prove useless in most instances because it would not have prior knowledge of the

planned disclosure. Third, most employees would probably find the requirement of signing such an agreement insulting and demeaning.

OPTION V: Include in the new Executive Order a section which will require the use of a uniform secrecy agreement and that all government employees execute such an agreement as a condition of obtaining access to classified information.

ADVANTAGES: The advantages will be the same as those in Option IV. However, this Option would probably have the added advantage of reducing legal problems in attempting to enforce the agreement because of its uniformity.

DISADVANTAGES: The disadvantages of this Option are the same as those in Option IV.

OPTION VI: Include in the new Executive Order a section which will require all government employees to execute a secrecy agreement as a condition to obtaining employment or continuing in their present employment.

ADVANTAGES: The advantages of this Option are the same as Option IV.

DISADVANTAGES: The disadvantages of this Option are the same as those in Option IV. It also has the disadvantage

that it could present legal problems in attempting to apply it to the military, career civil service entrants and present government employees.

OPTION VII: 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: The advantages of this Option are the same as Option IV. It could also add two additional deterrents through the liquidated damage clause or a civil fine requirement.

DISADVANTAGES: The disadvantages of this Option are the same as Option IV. It 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 probably 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.

RECOMMENDATION: The new Executive Order should include a section which will require all government employees to

execute a uniform secrecy agreement as a condition of obtaining access to classified information, whereby they agree not to publish, disclose or otherwise make available classified information to any unauthorized person. CIA concurs, but urge that the application of such an agreement be prospective only. DOJ dissents.

I. Working Group on Classification/Declassification

Chairman - Arthur F. Van Cook, DoD - 695 2686

Sub Group C/D-1

Chairman: Department of State representative [Jeffrey Smith] 632-9516

Composition: DoD, CIA, ERDA, Justice, Domestic Staff and NSA(Observer)
STAT [redacted] IC Staff, NSC

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

Points for Consideration:

- Should the new Order prescribe minimum criteria for classification of official information?
- Should the new Order prescribe policy prohibiting classification of certain categories of information or classification for certain purposes, i.e., to conceal inefficiency or administrative error, etc?
- What is "sensitive national security information"? Is the standard of E.O. 11652, i.e. "could reasonably be expected to cause damage to the national security" an adequate legal standard?
- Are the existing categories of E.O. 11652 (i.e. Top Secret, Secret, Confidential) meaningful? Should we re-define the categories, perhaps reducing them to two or increasing them to four?

- Should the new Executive Order establish special categories for information protected by statute, i.e., the DCI's responsibility for protection of intelligence sources and methods, and NSA's responsibilities for communications intelligence?
- Should the new Order prescribe rules which would bring about mandatory paragraph marking?
- What measures can be incorporated in the new Order to reduce the problem of overclassification, unnecessary classification and overuse of exemption authority?
- Should the Departments and Agencies prepare classification guidelines for their employees?

Sub Group C/D-2

Chairman: NARS representative [Allen Thompson] 523-3165 Rm 18W, NARS

Composition: State, OJCS, NSC and OMB

STAT [redacted]

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

Points for Consideration:

- Should the Departments and Agencies prepare declassification guidelines for their employees.
- Should more emphasis be placed on the Foreign Relations Series, or other Departmental publications, or on programs by the Archives to publish important papers?

Points for Consideration:

- Should the new Order require that Departments give emphasis to declassification comparable to that given to classification? In this connection, should the new Order require decentralization of declassification authority?
- Should the new Order establish criteria for declassification?
- * Can the automatic declassification system be modified or expanded to accelerate declassification or to reduce the amount of information that is exempted from automatic declassification? Are the periods for automatic declassification established by E.O. 11652 too long (i.e., 10 years for TS, 8 for S, 6 for C)?
- What can be done to increase the use of the automatic declassification system, or to use "specific event declassification," e.g., conclusion of a certain negotiation?
- * Should the new Order limit the authority of original classifiers to extend classification life beyond a particular period?
- Could the automatic downgrading by step be eliminated? (Is it meaningful to say that Top Secret automatically goes to Secret after two years?)
- Should the new Order provide for access to classified information for research purposes (former Presidential appointees), historical researchers, etc.)?

RECOMMENDATION I

That the Agency push for the retention of the present 30 year time frame for the systematic review of classified records. Should this prove impractical, then move for a compromise of 25 years.

THE AGENCY'S SITUATION

A reduction to a 20 year time frame would give the Agency a backlog of approximately 28,500,000* classified pages to review. (A 25 year limit would have a backlog of approximately 9,500,000* pages.) These figures do not take into account the existing backlog of 12,000,000 pages of OSS material (22.8% reviewed** but none released to the public since the records required by the Executive Order have not yet been prepared) or the estimated 1,000,000 pages of predecessor organizations (CIG, SSU, etc..).

In addition, the Records Review Branch (RRB) which is responsible for the Agency's review program, only came into existence on 2 May 1977. It is realistically expected that it will be another six months to a year before the unit is fully staffed and operational. And whether or not its proposed 40 man staff can keep up with the requirements of the 30 year time period is already open to debate.

* Numbers based on recent records survey which showed that there will be approximately 1,500,00 pages to review per year for the 1947-1950 period and approximately 3,500,000 per year for the period 1951-1956.

** Its taken a 15 man annuitant team three years to review 22.8% of the OSS records or 2,736,000 pages of the 12,000,000 total.

CONCLUSION

With its present resources, the Agency will be fortunate to meet the 30 year requirement. Should the time frame be reduced to 20 or 25 years, the Agency could only meet this new requirement by a large increase in its present allotted resources. When the final product is considered, one must question whether the additional expenditure required is worth it or not.

ADVANTAGES IN MAINTAINING A 30 YEAR LIMIT

a. To obtain and maintain the 30 year line will require little increase in present allotted resources.

b. The resulting flood of paper caused by a reduction in the time period would greatly increase the likelihood of an error.

c. A 20 or 25 year time frame would probably mean fewer records would or could be released to the public.

d. A 20 or 25 year time span might unnecessarily upset our foreign sources.

e. Finally, any increase in resources programmed for a declassification program means that CIA's primary function of gathering intelligence will suffer since these additional resources will undoubtedly come from these areas.

ADDITIONAL POINT

The CD-2 panel was also requested to consider that if the time frame was to be reduced to 20 (or 25 years), could the resulting backlog be completely reviewed in a 6 year time frame? Or a 10 year time frame?

ADDITIONAL CONCLUSION

The Agency not commit itself to a firm date when a review of backlogged records would be completed. As shown earlier, if the review time was to be reduced to 20 years, the Agency would then find itself with a backlog of approximately 28,500,000 pages. To expect to review this material, in addition to the material that would have to be reviewed annually, in either a 6 or 10 year time frame would be unthinkable. It is estimated that it would require 500 to 600 people to review the material in a 6 year period and 350 to 450 for the 10 year span. Simply a luxury the Agency could not afford. (And then there is the question of what you would do with these people when the review ended?)

The same would be true only to a lesser degree if a 25 year limit was chosen.

RECOMMENDATION II

That section 4 (C) of the current E.O. 11652 be retained in its present language. (Concerns foreign material.)

RECOMMENDATION III

That section 5(E)(1) be expanded to include protection for sources and methods as well as retaining the national security and the personal jeopardy provisions. Further recommend that the definitions for these items not be made more specific but remain in general terms.

RECOMMENDATION IV

Recommend that the Agency oppose any type of bulk declassification moves. RRB has been exploring this possibility and has yet to identify a single category where it is possible to release material without some sort of review. The closest thing yet identified was the FBIS material but even this had to be reviewed first.

In fact, recommend that the Agency go the opposite way and seek categories that might be exempted from review since they contain so much classified and sensitive material that declassification review would be pointless. An example here would be Agent 201 Files.

CONCLUSION V

Take out the proposed section concerning the State Department's Foreign Relations series. This is a special interest item which does not belong in an Executive Order on Classification and Declassification.

RECOMMENDATION VI

Recommend that a statement be included that only permanent records (as identified on approved record schedules) need be reviewed, regardless of their age. Example: records that are scheduled to be destroyed after 50 years would not be reviewed since it has been determined that they are not permanent records.

RECOMMENDATION VII

Recommend that a statement be included that working aids which are merely copies of other records be exempt from review. An example would be the filming of all cables within the Agency which are then held for reference purposes. This material should not be subject to review since it is merely a reference aid and the original cables will be reviewed when the files containing them are analyzed.

RECOMMENDATION VIII

Strong statement that one agency may not declassify records that effect the functions of another until the second agency has had an opportunity to review the documents.

Example is the CIA information turning up in material recently declassified by the Department of State.

RECOMMENDATION IX

Have the Director approve review guidelines and not the lists of documents reviewed (325 forms). Experience has already shown that this system is impractical since the Director is usually presented a list of several thousand documents and he really has no idea what he is signing.

Besides, the last list of material sent to the DCI's office for signature has been over two months in processing and has yet to be returned to RRB. Once the review program is fully geared, and when one considers the volume, such a time lag would be entirely unacceptable.

RECOMMENDATION X

That the current section 9 of E.O. 11652 be retained as written.

Also that section 8 of the current E.O. 11652 be expanded to include a statement covering CIA and the 1947 law requiring protection of sources and methods.

RECOMMENDATION XI

That section VII of the National Security Council Directive of 17 May 1972 be stricken. (Concerns data index information on records reviewed.)

To comply with this requirement, RRB has given ball park estimates of between 50-100 million dollars. While some sort of computer system will be required, believe this should be left to the individual agencies.

RECOMMENDATION XII

That the National Archives be tasked with the responsibility of identifying and marking duplicate copies of records already reviewed by an Agency based in the results of a previous review conducted by said Agency. This would apply, of course, only to files already accessioned to NARS.

Example: During a recent visit to the Suitland Records Center, a test produced the same CIA document in 42 different files. Personnel at Suitland further stated that had the time and effort been taken, the same document could probably have been turned up an additional 40 to 50 times.

This proposal would task NARS with the responsibility of identifying and acting upon any duplicate copies of documents once the first initial copy has been reviewed and its classification status determined. In other words, CIA reviewers would review the first copy of a document encountered and NARS would then be tasked with job of pulling and marking any additional copies of the same document in accordance with the Agency's review.

This would apply only to records already accessioned to NARS and which are thereby controlled by NARS.