

ROUTING AND RECORD SHEET

SUBJECT: (Optional) **Friday Meeting With Secretary Weinberger
Regarding Executive Order on Classification**

FROM:

 Deputy General Counsel

EXTENSION

NO. OGC 82-01703

STA

DATE 18 February 1982

TO: (Officer designation, room number, and building)

DATE

OFFICER'S INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

RECEIVED

FORWARDED

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	RECEIVED	FORWARDED	OFFICER'S INITIALS
ExDir																	
DDCI																	
DCI																	

NO REFERRAL TO OSD. WAIVER APPLIES

FEB 19 10 43 AM '82

OGC 82-01703
18 February 1982

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence

FROM: Deputy General Counsel

SUBJECT: Friday Meeting With Secretary Weinberger
Regarding Executive Order on Classification

STAT

1. The Secretary of Defense has proposed amending the draft Executive order on classification to protect certain technological data that he believes cannot be protected adequately under current standards.
2. The proposal was initiated to enable the United States to:
 - a. protect sensitive national security information, particularly militarily critical technology and operational data developed solely for the use of the Armed Forces;
 - b. prevent transfer of sensitive United States technology to foreign powers on a silver platter;
 - c. rectify a perceived inability under the current order to classify certain technological data;
 - d. facilitate dissemination and use of certain information by federal personnel and contractors by removing trustworthiness requirements and establishing only minimal controls over such data.

Specifically, the proposal (Tab 1) authorizes the Secretary of Defense to classify information expected to cause the United States to lose a military technological or operational advantage. As drafted, it:

e. authorizes the Secretary of Defense to classify information that if disclosed could cause the United States to lose a military technological or operational advantage;

f. allows classification without regard either to current classification levels or safeguarding and clearance requirements;

g. permits de facto creation of alternative classification scheme including lesser classification levels;

h. enables the Secretary of Defense to promulgate regulations binding on all agencies.

I support, in principle, the DoD proposal to ensure protection of technological data, but believe the approach raises serious problems that need to be resolved.

3. In my view the DoD proposal runs counter to the very essence of national security controls. Its adoption would dilute the classification order in that it contemplates providing classified information to noncleared personnel and authorizes widespread dissemination of classified data without regard to established safeguarding requirements. This attempt to "have it both ways," I believe, will result in a meaningless classification scheme. Our ability to keep technological information "classified" depends, at least in part, on the strength of our efforts to properly safeguard it.

4. Moreover, I believe the current draft Executive order does provide authority to protect such information adequately. The draft authorizes classification upon a showing that disclosure of information could damage the national security. Such damage would include, I believe, the loss of technological advantage. Trustworthiness requirements, which DoD would eliminate for such technological information, should be retained, but the current requirements offer sufficient flexibility to permit less stringent standards.

5. For this reason, I propose as an alternative that we cooperate with DoD to seek an amendment to the NSC directive implementing the order. That amendment could lessen, but not eliminate, safeguarding standards for sensitive but routinely used technological data. Since the current directive now contains a similar although more limited provision, my proposal is not likely to receive significant adverse reaction.

6. A more detailed review of the DoD proposal is attached for your information at Tab 2. It concludes, and I agree, that we should support DoD's objectives, but be wary of the approach.

STAT



Attachments:
As stated.

TAB 1

Add new Section 6.2(b) to read as follows:

(b) In the interest of the national defense, and notwithstanding the provisions of Sections 1 and 4, the Secretary of Defense is authorized to classify information the unauthorized disclosure of which reasonably could be expected to be prejudicial to the national security because it would cause the loss to the United States of a military technological or operational advantage. A classification designation other than as prescribed in Section 1.1 may be applied to such information. The Secretary of Defense shall promulgate regulations, that shall be binding on the agencies, providing that such information shall be safeguarded at a level lower than Confidential.

TAB 2

OGC 82-01641
18 February 1982

MEMORANDUM FOR:

[REDACTED]
Deputy General Counsel

STAT

FROM:

[REDACTED]
Assistant General Counsel

STAT

SUBJECT:

Background for DCI's Meeting With Secretary of
Defense on Classification Executive Order

1. The Secretary of Defense has proposed amending the draft Executive order on classification and intends to discuss that proposal with the DCI at their meeting on Friday. This memorandum summarizes the Secretary's objectives and this Agency's previous reaction, presents my views on the possible ramifications of the proposal, and offers several options for consideration. Because DoD did not send me the language it intends to raise with the DCI until this afternoon, I have addressed the previous proposal at greater length than I have discussed the new proposal. The same principles and concerns apply, however, and should be kept in mind when responding to the new DoD proposal. That new proposal provides:

6.2(b). In the interest of the national defense, and notwithstanding the provisions of Sections 1 and 4, the Secretary of Defense is authorized to classify information the unauthorized disclosure of which reasonably could be expected to be prejudicial to the national security because it would cause the loss to the United States of a military technological or operational advantage. A classification designation other than as prescribed in Section 1.1 may be applied to such information. The Secretary of Defense shall promulgate regulations, that shall be binding on the agencies, providing that such information shall be safeguarded at a level lower than Confidential.

2. Secretary Weinberger initially proposed a fourth level of classified information, called "Restricted," to be applied to

certain information, "particularly militarily critical technology and operational data developed solely for the use of our Armed Forces." Under that proposal (Tab A), the Executive order would continue the classification levels Top Secret, Secret, and Confidential, and further provide that:

"Restricted" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause the loss to the United States of a technological, diplomatic, intelligence, cryptologic, or military advantage and which requires protection in the interest of national security.

Defense is willing to omit the underscored language if State and CIA do not support the proposal. The Agency position to date has been essentially to support DoD in principle, while expressing reservations, both on legal and policy grounds, about the specific language proposed (Tab B).

3. The DoD position is based primarily on the premise that certain sensitive information related to the national security, particularly, although apparently not exclusively, information involving critical state-of-the-art military technology, cannot be protected under current classification standards. The proposal would enable the United States to protect a wide range of technical and training data, produced solely for use by the Armed Forces, upon showing that disclosure of the information could result in a loss of an advantage to the United States. The draft order now permits classification only upon showing a reasonable expectation of damage to the national security, and reflects a less stringent standard than that required to be met under the current order, namely, "identifiable" damage. However, this in itself seems to deflate the DoD argument that the additional classification level is needed to provide increased protection for sensitive technological information, for information that will cause the loss of a technological advantage and that requires protection in the interest of national security implicitly also would be expected to cause damage to the national security and warrant classification at the Confidential level. Moreover, section 1-302 of the new draft explicitly requires that information be classified if its release, when viewed in the context of other information, could be expected to damage the national security. This recognition of the so-called "mosaic" or "aggregate" approach should further alleviate Secretary Weinberger's concerns.

4. The proposal for further levels of classification is further intended to enable the Department to safeguard sensitive information while imposing only minimal controls within the government and defense industry communities. Under the current and proposed orders a person is eligible for access to classified information only if trustworthy and if access is essential for a government purpose (i.e., the person has a need-to-know). The Defense proposal would eliminate the trustworthiness standard and establish less stringent requirements for storing and handling Restricted information. For example, DoD suggests that Army field manuals describing the operational deployment of the LANCE missile could be provided to noncleared personnel and subjected to minimal safeguarding controls, but would be classified, for example, Restricted, provided to nonclerical federal and contractor personnel, and exempt from public release under the FOIA. Thus, for certain categories of classified information, as yet imprecisely defined, access determinations would be based solely upon an exhibited need for the information, without any consideration of the recipient's reliability.

5. While useful perhaps as a dissemination control, the DoD approach is inherently inconsistent with the well-established premise that information is to be classified, and provided limited distribution, because of the potential disadvantage to the national defense or foreign relations of the United States. Such a wholesale abandonment of traditional principles raises serious questions about the sensitivity of, and the ability to protect, information that will be provided without regard to trustworthiness standards. Also, this approach could result in improper use of the Restricted category by underclassifying to avoid the bureaucratic burdens involved in clearing personnel and storing material properly. To the extent the loss of information could result in the United States suffering a militarily technological loss, that information should be classified at least at the Confidential level and handled accordingly if public and judicial scrutiny and criticism are to be avoided. More importantly, dissemination of information controlled solely on a need-to-know basis could be insufficient to prevent entry of the information into the public domain.

6. These concerns arise less with the concept espoused by DoD than with the approach. The absence of any precise criteria for determining what constitutes a technological, diplomatic, intelligence, cryptologic, or military loss seems to present a fatal flaw. This not only could result in underclassification and disclosures to noncleared persons, but also could remove from the public domain considerable information developed by industry and now unclassified. There is no indication, for example,

whether Restricted technological data would be limited to data subject to export controls. If not, could persons who disclose such data to foreign powers nevertheless be prosecuted for providing "classified" information in violation of U.S. criminal laws? As drafted, the DoD proposal cannot resolve these concerns.

7. As stated, it is my view the DoD language as proposed is unnecessary. If, as DoD concedes, loss of certain information would be "demonstrably disadvantageous" to U.S. national security interests, that information can be classified under the draft Executive order. Technological matters, military plans, weapons and their capabilities, intelligence and diplomatic sources, and cryptology all are classifiable pursuant to section 1-301. Recognizing, however, the practical ramifications of the increasing need to protect technological information, the following alternatives are presented for your consideration:

OPTION A:

Seek a separate Executive order addressing the need to protect certain unclassified information from public disclosure.

Advantages:

- 1) Provides further opportunity to study the problem.
- 2) Avoids the trustworthiness issue.
- 3) Avoids dilution of classification standards.

Disadvantages:

- 1) Does not carry FOIA protection of classified information.
- 2) Avoids determining of classifiability of sensitive technological data.

OPTION B(1):

Support DoD's initial proposal to create a fourth level of classification, "Restricted," to cover technological, diplomatic, intelligence, cryptologic, and military information.

Advantages:

- 1) Recognizes desirability of protecting broad categories of sensitive data.
- 2) Eases administrative burdens imposed by clearance and safeguarding requirements.
- 3) Conforms U.S. system to NATO system using "Restricted" caveats.
- 4) Provides strong mechanism to protect sensitive data when doubt exists as to ability to classify.
- 5) Prevents giving technology away on a silver platter.

Disadvantages:

- 1) Unnecessary in view of classification standards under draft order.
- 2) Lacks precise guidelines or standards for identifying classifiable information.
- 3) Invites abuse by authorizing underclassification and dissemination to uncleared persons.
- 4) "Restricted" caveat easily confused with "Restricted Data" caveat under Atomic Energy Act.
- 5) Invites public criticism of undue government secrecy.
- 6) Probably will not be effective to prevent loss to hostile services.
- 7) Dilutes effectiveness of other classification categories.

OPTION B(2):

Support DoD's proposal, but limited to technological and military loss.

Advantages:

Same as B(1), plus less likely to receive so much public criticism in view of more limited scope.

Disadvantages:

Same as B(1).

OPTION C:

Amend draft Executive order to define "damage to the national security" as either a disadvantage to the United States or an advantage to a foreign power.

Advantages:

Permits classification of information covered by Defense's proposal at the Confidential level, but maintains trustworthiness standards and safeguard controls.

Disadvantages:

Permits overclassification, since foreign advantages can be relative (i.e., an advantage to one country may not be an advantage to another).

OPTION D:

Ensure NSC directive implementing the order provides limited waiver provisions governing security and safeguarding requirements.

Advantages:

- 1) Avoids amending the order and the problems that would entail.
- 2) Resolves DoD's practical problems in dealing with contractors.
- 3) Provides flexibility to clearly define extent of authorities.
- 4) Maintains traditional standards of classifiability.
- 5) Limited precedent exists in current directive.

6) Properly enables emphasis to be placed on dissemination controls rather than focus on classification levels.

Disadvantages:

- 1) Perceived as subversion of Executive order if waiver too broad.
- 2) Arguably lacks authority of Presidential order and, thus, less effective.

OPTION E (Tab C):

Adopt revised DoD proposal to permit the Secretary of Defense to establish guidelines to classify certain military technological and operational information.

Advantages:

- 1) Satisfies all DoD's concerns;
- 2) Limited in scope to sensitive technological information having military application, although language still too broad.
- 3) Consistent with provisions of the order enabling agency heads to create additional categories of classifiable information.
- 4) Sends appropriate message on U.S. policies and priorities.

Disadvantages:

- 1) In effect, permits Secretary of Defense to establish a new classification scheme.
- 2) Permits underclassification and does not resolve concerns with providing access to noncleared persons.
- 3) Appears to permit additional classification levels that contain the same defects as a Restricted category without being so explicit.

4) Amending order likely to invite further public or congressional scrutiny.

RECOMMENDATION: Options C and D.

8. Adopting both options C and D provides a dual benefit. First, as the order already permits classification of the information addressed by DoD, there is no need to effect any substantive change to the order. Clearly, certain technology losses can damage national security. In those cases, either when the damage places the U.S. at a disadvantage or gives a foreign power a technological gain, the data can be classified Confidential. A clear definition of "damage" helps ensure this result. Moreover, with that problem resolved, the practical concerns raised by Defense can be disposed of by having the NSC directive implementing the order authorize the Secretary, for clearly defined technological data -- perhaps based in part upon export laws -- provide limited waiver of the storage, dissemination and other safeguarding requirements. While the directive currently permits every agency head to do this to a limited extent, minor revisions can provide DoD, and CIA, the needed flexibility to disseminate routinely used, but sensitive, classified data with less chance of losing control over the information. Moreover, since trustworthiness standards are not defined even in the current order, ample flexibility appears to exist to provide routine information labeled, for example, "Confidential-Technical" to contractor personnel based only on a National Agency Records check. More importantly, this approach seems to eliminate the possible criticism that the government is improperly extending its cloak of secrecy into the private sector or that, on the other hand, national security standards are being diluted.

9. The new DoD proposal at option E appears to offer none of the advantages of options C and D. It is more narrowly drawn but needs further revision, and does not actually create a separate classification level but permits the Secretary of Defense to do so. Moreover, any national security classification system that does not require at least some trustworthiness standards would seem to be fatally flawed. I do not believe DoD can have it both ways; that it, we should not on the one hand attempt to restrict access to sensitive information in the interests of national security, while on the other hand decline to impose proper safeguards for that information because of the administrative burden that would be required to do so. This inevitably will result in a meaningless classification scheme and render us unable to keep the information "classified." Moreover, query the impact such a scheme would have on the ability to

prosecute under title 18 for the disclosure of "classified" information, or the ability to utilize the graymail legislation, when information is classified but no efforts have been made to properly safeguard it. These problems pose serious obstacles to the DoD proposals.

10. Absent adoption of these options, of course, is the possibility of taking no action to support Defense. In view of the merits of the DoD concept, however, that would not appear to be a viable option. I believe it would be useful to cooperate with DoD to draft acceptable language to protect sensitive technological information, whether that information involves military or intelligence equities, and I believe an amendment to the NSC directive offers the best opportunity of a worthwhile revision.

STAT



Attachments:
As stated

TAB A

JAN 18 2 07 PM '82



THE SECRETARY OF DEFENSE

WASHINGTON, THE DISTRICT OF COLUMBIA

U. S. DEPARTMENT OF DEFENSE

15 JAN 1982

82-01580

MEMORANDUM FOR ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS

SUBJECT: Executive Order on Classification

This is in response to the December 23, 1981 memorandum from the Counsellor to the President that requests that this Department's comments on the latest draft replacement for Executive Order 12065, "National Security Information" be provided to you.

While we can support much in the new revision, we note that only some 30% of previous DoD comments have been incorporated into this revised draft.

Of greatest concern is the failure to include in this current draft our previous proposal to establish a fourth level of classification, namely, "Restricted." We believe this omission is unfortunate. By its omission from the current draft, other departments and agencies of the Executive Branch will not have the opportunity to review and comment on its merits.

The existing three-level classification scheme has not provided adequate protection for a large body of sensitive national security information, particularly militarily critical technology and operational data developed solely for the use of our Armed Forces. The current uncontrolled dissemination of this sensitive information, especially when taken in the aggregate, is demonstrably disadvantageous to U.S. national security interests. The loss of such information and the consequent advantages gained by our adversaries require that steps be taken now to provide legal and positive control of it.

Of course, some will say that an added classification category will draw criticism that the revised Order increases the suppression of government information by broadening what can be classified and increasing the amount of classified information. While the number of classified documents will probably increase as a result of the fourth classification, this increase does not mean denial to the general public of information it needs to be informed. At issue is the establishment of a more equitable balance between open government and the government's responsibility

W00062

to secure the public interest. Restricting the public availability of scientific and technical data and, for example, Army field manuals describing the operational deployment of the LANCE missile, does not constrain information the public requires to be informed about the activities and operating functions of its government. Expansion of the current classification system should not be viewed as a radical departure but rather as a reasonable, necessary, and responsible extension of access control over certain information based on legitimate national security concerns. It is an immediate and proper solution to preclude further loss of such information.

While we are willing to limit the scope of the fourth level of classification to military technical and operational information, we believe it would be a serious and unfortunate mistake not to take this opportunity to help stem the flow of U.S. national security information that is now freely available and useful to our adversaries.

Attachment 1 contains a detailed rationale supporting the establishment of the fourth level of classification - RESTRICTED. The Department's other changes to the replacement order are contained in Attachment 2.

A handwritten signature in black ink, appearing to be 'Kup' or similar, is located in the center-right of the page.

Attachments

**Copy furnished:
Counsellor to
the President**

Defense Department Proposal to Establish the RESTRICTED Classification

Loss of U.S. technology is pervasive and uncontrolled. The unremitting flow of unclassified national security information to hostile nations, particularly technology and technical data with military application, is one of the more serious problems confronting this Administration. There is ample evidence that Soviet bloc acquisitions of unclassified national security related publications poses a considerable threat to the U.S. military posture and that of our allies. It greatly enhances our adversaries' capabilities to design, produce and field weapons systems of all types, as well as develop measures to counter U.S. weapons systems. It cuts their production costs, shortens their production times, and improves the quality of their product.

A Soviet scientist who defected several years ago told Congress that the majority of Soviet information collection requirements can be openly obtained in the United States. The FBI has estimated that as high as 90% of the Soviet collection requirements can be satisfied through open sources. We are painfully aware of Communist bloc efforts within the United States to obtain technology, most of which through legal means, which we are powerless to stop. Prior to February 1980, for example, we stood helplessly by as the Soviet Union purchased 80,000 technical documents each year from the National Technical Information Service (NTIS). Although their access to the NTIS has now been officially terminated, their surrogates continue to exploit this source of extremely valuable information.

Members of Congress, industry spokesmen, and the media frequently lament this state of affairs, and ask is there nothing that can be done. Unfortunately it has always been presumed that little could or should be done to limit such acquisitions, relying instead on the ability of the originators of such documents to properly secure sensitive information by using the existing security classification system. This is precisely the point of the Defense proposal. The existing three-level classification scheme has not provided adequate protection to a large body of sensitive national security information, particularly militarily critical technology and operational data developed solely for the use of our Armed Forces.

Classification of such information under the current three-level system has been neither possible nor practical. Although such sensitive national security information fits the categories permitted to be classified, it does not rise to the level of the "identifiable damage" standard prescribed by the current Order, nor does it rise to the "damage" standard of the draft revision. Disclosure of the technical characteristics of electronic components used in a missile guidance system, for example, may not appear to damage the national security, and yet may well provide our adversaries with precisely what they need to produce a more effective missile. It is this "damage" standard that is applied

Attachment 1

by originators in deciding whether to make their documents unclassified or to protect them by security classification.

At the practical level, there is also need to permit defense components, contractors, and other government entities to freely utilize and exchange information of this nature without the costs and delays entailed by safeguarding requirements imposed under the current three-level system. Using the previous example, if the technical characteristics of the electronic components were classified under the provisions of the present Order, no one could handle them or have access to them without a security clearance; they could not be stored or transmitted except by approved means; and they could not be discussed except over secure communications. Under the current system of classification, technical information of this sort is frequently not classified because the owner of the information believes his need to freely utilize it takes precedence over whatever advantage the United States might lose if the information were disclosed to our adversaries. He might well be right, but the legal consequence of his decision is to make the information available under a variety of circumstances such as the Freedom of Information Act; through government distribution centers; discussion in industry marketing brochures, presentations, and meetings; through the Federal Depository Library System; through the International Exchange Program; speeches; cultural and trade exchanges.

It is to remedy this situation -- to make possible control over dissemination of technical information without at the same time creating a system that would unduly inhibit the defense industrial process -- that DoD has proposed the fourth level of classification. It would allow us, and other agencies, to classify information useful to our adversaries, enabling us to keep it out of public dissemination channels while at the same time subjecting it to minimal controls within the federal government and defense industry communities. As we conceive it, the only requirement for access to RESTRICTED would be a legitimate need for it in the performance of official government functions. No background investigation would be required prior to granting access. Storage and handling requirements would similarly be minimal to prevent persons who had no official need for the information from obtaining access to it.

Some may argue that a fourth level of classification would dilute the efficacy of the security classification system resulting in a loss of its credibility. Quite the contrary, the fourth classification level strengthens the system by authorizing the protection of valuable national security information that is now jeopardized because "nothing can be done about it under the current Order. It recognizes a serious information control problem and provides a credible solution. The "damage" standard remains undiluted for the higher levels of classification; the fourth classification level introduces a realistic "loss" standard for the protection of sensitive national security information that is now unprotected; and the overall classification protection of information in the interest of national security is strengthened. Expansion of the current classification scheme will not be viewed as a radical departure

but rather as a reasonable, necessary, and responsible extension of access controls over information based on legitimate security concerns.

Most of the NATO member nations and NATO itself use a four-level security classification system to include the classification "Restricted." The incompatibility of the U.S. three-level system with NATO and many countries outside of NATO continually creates operational problems having an adverse effect on NATO interoperability and standardization. These and other persistent problems would be resolved with the establishment of "Restricted" as a U.S. security classification.

Alternatives put forth to accomplish such increased controls, such as amending the FOIA or existing statutes governing export control fail to recognize the duty and authority to protect national security information which clearly resides with the President.

Other alternatives, such as increased emphasis on dissemination control systems by individual agencies or through additional Executive orders, do not have the force or immediate effect of security classification. Nor would such controls, under existing legislative policy, be sufficient to effectively stem the flow of sensitive national security information to hostile nations.

We want to make clear this additional category of classification is not intended to preclude any greater public awareness of defense activities, operations or policy than is now possible. We emphasize our purpose is solely to protect certain information by subjecting its dissemination through open channels to greater control. We want to deny our adversaries the proverbial "silver platter" they now have. Private firms and individuals in the United States who need this information to continue to do business with the Government will continue to get it, but through official channels rather than sources available to the general public.

It is my understanding that other Executive Branch agencies are reluctantly distributing and releasing information that is disadvantageous to U.S. national security interests. It was for this reason that we included in our proposed definition of Restricted loss of a "diplomatic" or "intelligence" advantage. However, if State and CIA do not share the same degree of concern over loss of such information as we do over military technology and operational information then we would offer the following more narrow definition for Restricted information as an alternate proposal:

"Restricted" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause the loss to the United States of a technological or military advantage and which requires protection in the interest of national security.

This alternately defined fourth classification level would apply to a wide range of technical and training data produced by this Department

which does not meet the current criteria for classification. This information, invaluable as a reflection of the state-of-the-art of military technology and the extent to which it has tactical and strategic military application is highly sought and easily obtained by our adversaries. Several highly classified studies can be provided that demonstrate the degree to which our adversaries are using such information to their immediate and long-range benefit. However, the benefit of the alternative proposal principally accrues to this Department since it is the primary and largest user of technology related and military operational information.

The current uncontrolled dissemination of sensitive but unclassified national security information, especially when taken in the aggregate, is demonstrably disadvantageous to U.S. national security interests. The loss of such information and the advantages gained by our adversaries requires that steps be taken now to provide legal and positive control of it. We continue to urge approval of our initially proposed fourth level of classification as an effective and inexpensive means to restrict access to sensitive national security information that is now unprotected. While we would accept the proposed alternate, more narrow definition that ameliorates some of this Department's concerns, we continue to believe that the problem of inadequate protection of sensitive national security information extends throughout the Executive Branch. There are no other acceptable alternatives if we are to discharge effectively our considerable responsibility for the protection of information in the interest of national security.

Changes to the revised order necessary to establish the RESTRICTED classification are as follows:

Change Section 1-101 to read:

1-101. National security information...shall be classified at one of the following [three] four levels:

Add Section 1-101(d) to read:

1-101(d). "Restricted" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause the loss to the United States of a technological, diplomatic, intelligence, cryptologic, or military advantage and which requires protection in the interest of national security.

Change Section 1-302 to read:

1-302. Information...shall be classified when...its unauthorized disclosure reasonably could be expected to cause the loss of an advantage to the United States or cause damage to the national security.

Change Section 1-501(d) to read:

(d) one of the [three] four classification designations....

Change Section 4-101 to read:

4-101. A person is eligible for access to Restricted information only when such access is essential to the accomplishment of authorized and lawful Government purposes. A person is eligible for access to [classified] Top Secret, Secret, or Confidential information only after a [formal] favorable determination of trustworthiness....

TAB B

81-98812

CENTRAL INTELLIGENCE AGENCY
WASHINGTON, D.C. 20505

OIS Registry

No: E.O. 12065

13 NOV 1981

Mr. Arthur F. Van Cook
Director of Information Security
Office of the Deputy Under Secretary of
Defense for Policy Review
Department of Defense
Room 3C260
Pentagon
Washington, D.C. 20301

Dear Mr. ^{Art} Van Cook:

We share the concern, expressed in your letter of 19 October 1981, for protecting certain information that does not meet the current criteria for classification under Executive Order 12065. In particular, we believe that advanced U.S. technology relating to national security systems should be afforded protection. The proposal to provide this protection by adding "RESTRICTED" as a fourth level of classification, however, raises several questions that we feel should be resolved before we can fully support this approach.


As you know, the 16 October 1981 Information Security Oversight Office (ISOO) draft replacement for Executive Order 12065 enhances the ability of the U.S. Government to protect technological information even without the addition of a new classification level. For example, Section 1-101(c) no longer would require a showing of "identifiable" damage to the national security in order to classify information. Section 1-103 no longer would require that information not be classified if there is reasonable doubt as to whether it should be. Section 1-302 would require explicitly that information be classified if it is an element of what has been referred to as the "aggregate" or "mosaic". And Section 1-401 no longer would require that a maximum duration of classification be set when information is classified.

Given these changes to Executive Order 12065, we believe that the proposal to add a "RESTRICTED" classification could in some cases result in information being provided less protection than it warrants. The new classification level easily could become a "catchall" for information that in many cases should and could be classified Confidential. We believe, for example, that a loss of advantage to the U.S. resulting from the disclosure of technological information relating to the national security would indeed damage the national security, and therefore such information should be classified at least Confidential.

Classifying information "RESTRICTED" rather than Confidential would be of particular concern in light of the proposal that access to such information would require only need-to-know and would not require a security clearance. While "RESTRICTED" information may be protected from public disclosure under the Freedom of Information Act, dissemination controlled only by need-to-know would be inadequate to prevent entry into the public domain. With the positive approach to classification reflected in the ISOO draft replacement for Executive Order 12065, we should be able to protect against loss of advantage to the U.S. through general understanding and increased utilization of classification in the aggregate. This would avoid possibly throwing the entire national security classification system open to question by the inclusion of information that does not require a determination of trustworthiness before granting access.


We are hopeful that the above questions might be resolved through a reformulation of the "RESTRICTED" proposal that would include a requirement for a determination of trustworthiness consistent with the existing three classification levels. Alternatively, we might support an effort to establish a basis for protecting technological information through legislation or a separate Executive order addressing the need to withhold certain unclassified information from public disclosure. We would be happy to meet with you and other interested parties to explore such alternative approaches to avoiding the loss of advantage to the U.S. resulting from premature disclosure of sensitive information.

Sincerely,


 Director of Information Services
 Directorate of Administration

STAT

DDA/OIS

 (13 November 1981)

STAT

Distribution:

Original-Addressee

2-OIS Subject Chrono

1-RSB Subject: Classification Mgt/EO 12065 Revision

1-RSB Chrono

TAB C

Add new Section 6.2(b) to read as follows:

(b) In the interest of the national defense, and notwithstanding the provisions of Sections 1 and 4, the Secretary of Defense is authorized to classify information the unauthorized disclosure of which reasonably could be expected to be prejudicial to the national security because it would cause the loss to the United States of a military technological or operational advantage. A classification designation other than as prescribed in Section 1.1 may be applied to such information. The Secretary of Defense shall promulgate regulations, that shall be binding on the agencies, providing that such information shall be safeguarded at a level lower than Confidential.