BY THE COMPTROLLER GENERAL

Report To The Congress

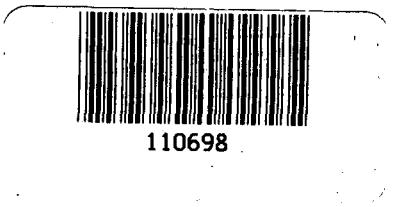
OF THE UNITED STATES

Continuing Problems In DOD's Classification Of National Security Information

Some individuals at DOD did not comply with the provisions of the 1978 Executive order and DOD's regulation on the classification of national security information. As a result, there was improper use of classification authority, improper classification of information, and deficiencies in the marking of classified information.

To correct these conditions, DOD should expand the training given to classifiers and improve its independent inspections of classification activities.

This report was prepared at the request of two congressional committees.



LCD 80 16
OCTOBER 26, 1979

COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-179296

CW0000001

To the President of the Senate and the
Speaker of the House of Representatives

This report describes the results of our review of classified documents at 23 military installations and offices in the continental United States, Hawaii, Europe, and the Canal Zone. It is the second in a series of reports on the classification of national security information. Our first report, "Improved Executive Branch Oversight Needed for the Government's National Security Information Classification Program," was issued March 9, 1979.

We are sending copies of this report to the Director, Office of Management and Budget; the Administrator of General Services; and the Secretary of Defense.

AGC00270
AGC00017
AGC00005

Comptroller General
of the United States

COMPTROLLER GENERAL'S REPORT TO THE CONGRESS

CONTINUING PROBLEMS IN DOD'S CLASSIFICATION OF NATIONAL SECURITY INFORMATION

D I G E S T

The Department of Defense (DOD) has continuing problems with its national security information classification program. They include

--improper use of classification authority,

--improper classification of information, and

--deficiencies in marking classified information.

GAO found such problems with 49 percent of the documents it reviewed at 23 DOD installations and offices in the continental United States, Hawaii, Europe, and the Canal Zone.

IMPROPER USE OF CLASSIFICATION AUTHORITY

Executive Order 12065, which governs the classification program, specifies the individuals authorized to originally classify information, when that authority may be delegated, and individuals authorized to classify information for periods longer than the normal 6 years. GAO found that

--information was originally classified by individuals who were not authorized classifiers;

--individuals with top secret classification authority improperly delegated authority to subordinates to extend classification for more than 6 years; and

--sections of some classification guides did not specify the level of classification to be used in classifying information on a derivative basis which, in effect, allows

unauthorized individuals to make original classification decisions. (See p. 5.)

IMPROPER CLASSIFICATION OF INFORMATION

Of 556 documents reviewed by GAO, 133, or about 24 percent, contained information that had been improperly classified. GAO found that

--information not related to national security was classified;

--references to classified documents that did not disclose classified information were classified;

--contrary to the order, when there was doubt as to the level of classification to be used, the more restrictive classification was used;

--the same information was classified inconsistently; and

--information that had lost some of its sensitivity was not downgraded. (See p. 12.)

DEFICIENCIES IN MARKING CLASSIFIED INFORMATION

Despite the fact that the current order and implementing instructions, as did the previous order that was in effect from 1972 to 1978, clearly specify the markings that are to be shown on each classified document, improper marking continues to be a problem for DOD.

Overall, GAO identified one or more marking errors on 33 percent of the documents it reviewed. The major marking deficiencies were that classified documents did not show the

--original classification authority or office of origin;

--date or event for declassification or review or the reason for classifying information for more than the standard 6-year period; and

--portions of information that were classified and unclassified. (See p. 19.)

The order requires that documents be portion marked so that the level of classification of information can be easily ascertained. GAO believes that, at least in the case of DOD, portion marking should also be used to identify specific information that requires protection for more than 6 years. Such markings would make some information available to the public at an earlier date and would facilitate the review and declassification of other information at a later date. (See p. 22.)

IMPROVED TRAINING AND INSPECTIONS NEEDED

Improved training and inspections are needed to reduce deficiencies in DOD's classification program.

Most classifiers told GAO that their training had generally consisted of orientation briefings for newly hired or transferred staff; periodic security briefings; and memorandums, newsletters, posters, and other security-awareness type publications. Training generally focused on physical safeguards and proper marking of information, rather than proper classification.

Similarly, inspections seldom, if ever, included an evaluation of whether information had been properly classified. As with training, inspections generally focused on physical safeguards and proper marking of information. Most classifiers indicated that GAO's review was the first time they had been asked by an independent party to justify their classification decisions. Neither the order nor the implementing instructions contain requirements or

guidance concerning the frequency or the types of inspections that are to be made. (See p. 25.)

RECOMMENDATIONS

The Secretary of Defense should revise DOD's information security program regulation to:

--Require all classification guides and instructions and revisions to be reviewed during periodic independent classification inspections. Unresolved deviations from the order and regulation should be brought to the attention of the Director of Information Security to assure prompt resolution.

--Require classified documents to be portion marked to identify information that requires protection for more than 6 years.

--Provide expanded training for individuals who classify information, originally or derivatively, to concentrate on, among other things (1) their responsibility to comply with the order and instructions, (2) who can classify information, (3) what information is to be classified, and (4) how to properly classify and mark information.

--Provide definitive guidance on the frequency of different levels of inspections that should be made and the items to be covered, with special reference to the need to question the propriety of classification decisions.

AGENCY COMMENTS

DOD believes that the errors described in the report were generally minor in nature and were the result of classifiers being unfamiliar with requirements of the new Executive order. DOD said that the reported discrepancies do not convey nor support a premise of noncompliance with the order, but do underscore the continuing need for management support for education and training efforts.

In commenting on GAO's recommendations, DOD said that it would consider having unresolved classification guide problems brought to the attention of the Director of Information Security for resolution, and providing guidance on the minimum frequency for security inspections and areas to be covered. DOD did not agree that classified documents should be marked to identify the portions that require protection for more than 6 years or that its regulation be revised to provide for expanded training. GAO still believes its recommendations concerning training and portion marking material requiring protection for longer than 6 years have merit. GAO believes its findings clearly demonstrate the need for expanded training, and portion marking would facilitate declassification at an earlier date. (See app. I and pp. 11, 18, 24, and 29.)

Contents

ABBREVIATIONS

GAO	General Accounting Office
DOD	Department of Defense

CHAPTER 1

INTRODUCTION

This review was requested by the Chairmen, Subcommittee on Priorities and Economy in Government, Joint Economic Committee, and the Subcommittee on Government Information and Individual Rights, House Committee on Government Operations.

The classification of national security information has been governed by various Executive orders since 1940. Implementation of the classification program is governed by Executive Order 12065, which took effect December 1, 1978. It superseded Executive Order 11652 which was in effect from June 1972 through November 1978. Both orders provide for three levels of classification--top secret, secret, and confidential--depending on the degree of sensitivity of the information to national security.

The previous order required the use of a general declassification schedule of 6 to 10 years for the automatic downgrading and eventual declassification of information, depending on its level of classification. The new order abolishes the general declassification schedule and limits the classification of most information to 6 years. It further provides that information requiring protection for a longer period can be classified for up to 20 years. Information constituting permanently valuable records of the Government must be reviewed for declassification at the end of 20 years, but classification can be extended for additional 10-year periods, provided the information is reviewed at the end of each 10 years. Foreign government information may be classified for up to 30 years.

The previous order allowed material to be exempted for 30 years before requiring a declassification review, and classification beyond that period could be extended indefinitely at the discretion of the head of the agency originating the document. Both orders provide that the exemption privilege be exercised only by an individual with the authority to originally classify top secret information and that it be used sparingly, consistent with national security interests.

The National Security Council was responsible for monitoring implementation of the previous order. An Interagency Classification Review Committee, composed of representatives from various Government agencies, assisted the Council. The Committee was responsible for ensuring compliance with the order and implementing directives issued by the President

through the Council. The new order makes the Administrator of General Services responsible for implementing and monitoring the program, and it directs him to delegate that responsibility to an Information Security Oversight Office.

Although the Department of Defense (DOD) has been using classification guides for many years, the new order is the first to specifically authorize their use. A classification guide should specify the level and duration of classification for specific types of information for a weapon system, project, or subject.

The classification of information is divided into two categories--original and derivative. An original classification is an initial determination that information, in the interests of national security, requires a specific degree or level of protection against unauthorized disclosure. A derivative classification occurs when classified information is extracted or summarized from one document for use in another. In other words, the classification assigned to the latter document is derived from the classification status of the former. Executive Order 12065 expands the use of derivative classification to include information that is classified based on directions included in an approved classification guide. Classification guides have to be approved in writing by the head of the agency or by an official with top secret classification authority.

In both orders the President has designated the heads of certain agencies and officials of those agencies to be authorized classifiers. Some agency officials have top secret authority, while others, depending on their need for such authority, have secret or confidential. Both orders have attempted to reduce the number of authorized classifiers on the assumption that such action would reduce the number of documents unnecessarily classified.

DOD classifies more information than any other Government agency. DOD is currently using 1,048 classification guides and hundreds of directives, instructions, and letters that are used as guides. DOD's information security program is governed by Information Security Program Regulation 5200.1-R, dated December 1978.

SCOPE OF REVIEW

Because of the size of the Government's national security information classification program the review is being done in phases. A report (LCD-78-125, Mar. 9, 1979) on the

first phase of our review discusses the need for improved executive branch oversight of the program. This report on the second phase of our review evaluates DOD's classification activity.

We visited 23 DOD installations and offices within the following organizations in the continental United States, Hawaii, Europe, and the Canal Zone:

--Office of the Secretary of Defense.

--Office of the Joint Chiefs of Staff.

--Department of the Army.

--Department of the Navy.

--Department of the Air Force.

We reviewed Executive Orders 11652 and 12065 and their implementing directives and instructions as well as DOD regulations and instructions relating to security classification practices. We also inquired about the development of classification guides for specific projects and systems.

To evaluate DOD's classification program, we selected and reviewed 556 top secret, secret, and confidential documents for proper classification by comparing the documents with the classification guide or the originally classified document. On 49 percent of these documents we found one or more errors pertaining to improper use of classification authority, improper classification of information, and improper marking that are described in the following chapters. We also discussed the rationale for such classification with security managers and classifiers.

We did not examine any information protected under DOD's special access programs. These programs control the access, distribution, and protection of particularly sensitive information. Hundreds of special designations are added to top secret, secret, and confidential classification markings that further limit access to information because special clearances are needed.

One DOD official said he believed that most top secret documents had special access caveats attached. There were thousands of classified documents within the intelligence field alone that were not subject to our selection for review because they also contained special access designations.

We did not determine the extent of these special access programs and the number of special clearances required to gain access to them because, until recently, these programs had not been centrally controlled. Executive Order 12065 has recognized this problem and has required agencies to establish a central control over these programs. At the time of our review, DOD had a study underway to comply with this requirement.

Our review of classified documents was hampered by the refusal of the Office of the Joint Chiefs of Staff and the Air Force to make certain documents available. DOD stated that certain documents that we requested were not made available to us because they dealt with Joint Strategic planning, and that access to such documents is severely restricted. DOD states that documents requested at the Air Force were denied to us because they were either originated by or responses to the Office of the Joint Chiefs of Staff and the Defense Intelligence Agency and could only be released by those organizations. Further, DOD does not believe that our review was hampered by these restrictions.

Since these two components did make other documents available, we did not pursue the matter. We do not know, however, if a review of the withheld documents would have disclosed deficiencies different from those found on the documents that were furnished.

Many of the documents denied to us by the Air Force were neither originated by nor in response to the Joint Chiefs of Staff or the Defense Intelligence Agency; rather, they were Air Force documents that merely contained references to documents from organizations outside the Air Force. We were told that any document created outside the Air Force, no matter how routine or mundane the subject area, would not be made available to us without approval by the originating agency. At one Air Force location visited, officials told us that this encompassed most of their documents.

CHAPTER 2

IMPROPER USE OF CLASSIFICATION AUTHORITY

Executive Order 12065 specifies (1) the DOD officials authorized to originally classify information and the circumstances when that authority may be delegated, (2) that only officials with top secret classification authority can classify information for periods longer than 6 years, and (3) the types of explicit instructions that should be included in classification guides used by individuals who classify information on a derivative basis. Notwithstanding the specificity of this guidance, we found that

- --information was originally classified by individuals who did not have original classification authority;
- --authority was improperly delegated to individuals to extend classification for more than 6 years; and
- --sections of some classification guides did not specify the level of classification to be used by individuals classifying information on a derivative basis, in effect making their classification decisions unauthorized original classification decisions.

INFORMATION CLASSIFIED BY INDIVIDUALS WHO WERE NOT AUTHORIZED CLASSIFIERS

The order designates the Secretaries of Defense, the Army, the Navy, and the Air Force as top secret classifiers and permits them to delegate authority to classify information to principal subordinate officials who have a frequent need for it. The order also provides that secret and confidential classification authority may be delegated to subordinate officials who have a frequent need for such authority. DOD's information security regulation requires that if an individual who is not an authorized original classifier, originates or develops information that the individual believes should be classified, the individual should mark the information with the intended classification and transmit it to an individual with classification authority for review and approval. The previous Executive order and its implementing instructions, in effect until November 30, 1978, contained similar provisions.

Of 556 documents reviewed at 7 locations, we identified 21 documents that were classified by individuals without original classification authority. These individuals did not have their decisions reviewed by someone with proper authority.

--Thirteen of these documents, classified by individuals without original classification authority, were ostensibly classified on a derivative basis citing a classification guide or other source document as the classification authority. However, the justification for each classification decision was not supported by the source documents cited as authority. Most individuals acknowledged that the derivative classification decisions were actually original decisions, even though a guide or some other material which discussed the subject area was cited. At one location, we were told that this was done for eight documents so that approval would not have to be obtained from an original classification authority. For example, at that location a message concerning a shipment of electronic equipment was classified confidential and a guide was cited as the basis for the classification. The individual who classified the message could not identify the section of the guide that supported his action. He told us that the classification was actually based on his own experience.

--Eight documents cited an individual or organizational position rather than a guide or other source material as classification authority. These documents were classified by individuals without original classification authority and were not reviewed or approved by someone with original classification authority. For example, one individual, who was not an authorized classifier, classified as confidential a report on a military exercise and cited his superior officer, who was an authorized classifier, as the classification authority. He said that he did not get his classification decision reviewed by his superior officer because he did not realize that it was necessary.

INDIVIDUALS IMPROPERLY DELEGATED AUTHORITY TO EXTEND CLASSIFICATION BEYOND 6 YEARS

The order allows only officials with top secret classification authority and certain agency heads to classify information for more than 6 years from the date of original

classification. The order states that "this authority shall be used sparingly."

Of the 556 documents we reviewed, we were able to identify 524 that had a date for declassification or review. We could not identify the declassification or review date on the other documents because those markings were missing or we did not obtain the cover sheet containing the declassification data. Of these 524 documents, 313, or 60 percent, were classified for longer than 6 years.

--In a December 28, 1978, memorandum, an individual with top secret authority designated 31 of his subordinates (most of whom were geographically located elsewhere) to use his position and title as classification authority for extending classification beyond 6 years. We obtained a copy of this memorandum on April 2, 1979. DOD officials later told us that this memorandum was in the process of being rescinded at that time. On May 10, 1979, the issuing office rescinded the December 1978 memorandum and replaced it with a classification guide. The authority to use this guide to extend classification of specific categories of information beyond 6 years is limited to the same 31 subordinates delegated authority in the December 28, 1978, memorandum. However, the guide is written so that (1) certain categories of information are taken almost verbatim from DOD's information security regulation without explaining what specifically within those categories requires extended protection, (2) only the minimum level of classification for categories of information is established, leaving the exact designation to the judgment of the user, and (3) only the maximum time those categories of information can be classified is specified, allowing the user to decide the specific duration of classification. We brought these deficiencies in the classification guide to the attention of DOD's Information Security Office in June 1979. (The problems with guides written in this manner is discussed in the following pages.)

--Another DOD organization specified in writing on April 12, 1979, 17 items of information that should be classified longer than 6 years. This authorization to extend classification for the specified items was delegated to at least 20 individuals within that organization. On April 25, 1979, we informed officials

of the organization that we believed the delegation of authority to extend classification beyond 6 years was contrary to the Executive order which prohibits the redelegation of original classification authority. Officials believed that delegating authority to extend classification beyond 6 years was necessary because it was unrealistic to expect the commanding officer (the only individual with top secret classification authority) to review all such documents to determine whether to extend classification. On June 21, 1979, an official from that organization told us that the April 12 memorandum would soon be rescinded and that instructions contained in it would be incorporated in a classification guide. As of October 1, 1979, that guide had not been issued. We do not know if use of the guide will be limited to the same individuals who had been delegated authority to extend classification. If use of the guide is not limited to those individuals, then anyone using that guide could extend classification for more than 6 years and be in compliance with the Executive order. Of course, the guide must state the reasons why the information has to remain classified for more than 6 years and it must be approved by the agency head or by an official with top secret classification authority.

CLASSIFICATON GUIDES PERMIT ORIGINAL CLASSIFICATION DECISIONS BY INDIVIDUALS NOT AUTHORIZED AS ORIGINAL CLASSIFIERS

Sections of some classification guides permit the users to decide the level of classification to be used for specific items. Since the majority of individuals who use guides in DOD do not have original classification authority, their decisions in selecting the appropriate level of classification, in effect, are original classification decisions.

The new Executive order authorizes the use of classification guides and provides that individuals using them as their authority for applying classification markings are derivatively classifying national security information, and therefore, do not have to be authorized as original classifiers. The DOD regulation states that guides used to direct derivative classification shall specifically identify the information to be classified and indicate how the designations, time limits, markings, and other requirements of the Executive order are to be applied to the information. The regulation further provides that classification guides shall

state which of the classification designations (i.e., top secret, secret, or confidential) applies to the information.

Implementing instructions issued by the Information Security Oversight Office on October 5, 1978, provide that each classification guide is to be kept current and is to be reviewed at least once every 2 years. The instructions do not state who is to make the review. DOD's regulation requires the originator of the guide to make the review. The regulation further provided that all guides issued before December 1, 1978, were to be reviewed and updated to meet the requirements and provisions of the regulation. That review was to be completed before December 1, the effective date of the new Executive order. While the regulation provides for the distribution of guides and revisions to various DOD offices, it does not require that the guides be reviewed by anyone other than the originator.

Of the 556 documents reviewed, 152, or 27 percent, cited guides as the authority for the classification. We examined 44 guides or portions thereof and found that at 13 locations 18 guides contained one or more items for which a level of classification was not specified. Selecting the proper level of classification was left to the discretion of the guides' users. For example:

--One classification guide contained at least three different items of information, ranging from unclassified to secret, without making it clear which level to use. The decision was left to the judgment of the user.

--Another guide that listed 53 different items of information provided a choice when 16 of the items are classified. For one item of information the range was from confidential to top secret. For six other items the guide allowed the classifier to choose unclassified or confidential. The guide instructed the user that "the level of classification will depend upon the classifier's judgment of the impact of the specific development on national security interests."

CONCLUSIONS

The above examples indicate that individuals responsible for classifying information believed that administrative convenience was sufficient reason for not complying with the explicit requirements of the Executive order and implementing instructions.

At 7 of the 23 locations visited, some individuals originally classified information even though they were not authorized to do so. Their actions, as well as those of individuals who improperly delegated authority to subordinates to extend the classification of information for more than 6 years, illustrates the need for DOD to emphasize the importance of compliance with the requirements pertaining to proper use of classification authority. Those requirements were established to preclude overclassification and underclassification of information relating to the national security.

Because of the size of DOD's classification program and the tremendous volume of information being classfied, we realize that it is not possible to entirely eliminate errors in judgment; however, we believe that the incidence of such errors could be reduced by improved training and independent inspections of classification operations. Our recommendations covering these points are included in chapter 5.

The use of classification guides that lack specificity and require the users to determine the level of classification to apply to certain items of information is not the intent of the Executive order nor DOD's regulation.

We concur with the provision of the DOD regulation that requires the originators of guides to review them at least once every 2 years for currency and accuracy, since they generally would be the ones most knowledgeable on the subject matter of the guides. However, we believe that someone other than the originators should also review the guides for compliance with the provision of the regulation; that is, that the level of classification is specified and that classification for longer than 6 years is properly justified. In our opinion, such independent reviews should minimize the possibility of the use of guides that allow original classification decisions to be made by individuals who have not been designated as original classifiers.

RECOMMENDATIONS

We recommend that the Secretary of Defense revise the information security program regulation to require that all classification guides, instructions, and revisions be reviewed during periodic, independent classification inspections to assure compliance with the provisions and intent of the Executive order and the DOD regulation. We further recommend that unresolved deviations from the requirements of the order

or the regulation, noted during these independent inspections, be brought to the attention of the Director of Information Security to assure their prompt resolution.

DOD COMMENTS AND OUR EVALUATION

On October 5, 1979, the Deputy Under Secretary of Defense commented on our findings and recommendations. (See app. I.) In commenting on our finding about the individual with top secret classification authority who gave 31 subordinates permission to extend classification for more than 6 years (see p. 7), DOD states that in July 1979 the Director of the Information Security Office requested that the May 1979 classification guide be revised to overcome its weaknesses. The prompt corrective action by the Director is commendable and we believe that if his suggestions are properly implemented, they will correct the guide's deficiencies. As of October 1, 1979, however, the Director had not been notified that the changes had been put into effect.

In response to the second example on page 7, DOD believes that if the correspondence specifying 17 items of information that should remain classified for longer than 6 years was signed by an official with top secret classification authority, "the correspondence was in effect a security classification guide within the meaning of the Executive Order." In our opinion, the correspondence cannot be considered a guide because it does not meet the criteria established by the order or DOD's information security program regulation. The correspondence does not specify the level of classification applicable to each item of information that requires extended protection, the duration of classification for each item, or the reasons for the extended protection.

As noted in DOD's comments, our recommendation has undergone minor revision to include classification guides and instructions (such as the correspondence described above) and to specify when the independent review should be made. Although DOD states that a review of classification guides by someone other than the originator is already common practice, we believe the fact that 18 of the 44 guides that we reviewed did not meet the established criteria necessitates formalizing the independent review requirement in DOD's information security program regulation.

CHAPTER 3

IMPROPER CLASSIFICATION OF INFORMATION

Both Executive orders and the various implementing instructions describe the types of information that should be classified for national security reasons--to preclude overclassification and underclassification and to make information about the Government available to the maximum extent possible. Nevertheless, we identified examples of improperly classified information at each DOD installation and office visited. Of the 556 documents reviewed, 133, or about 24 percent, contained one or more examples of improper classification. None of these cases involved classified information which was incorrectly treated as unclassified.

The following are some of the more significant problems noted.

--Information not related to national security was classified.

--References to classified documents were classified.

--The same information was classified inconsistently.

--Information that lost some of its sensitivity was not downgraded.

--When there was doubt about the level of classification, a higher classification level was assigned.

INFORMATION NOT RELATED TO NATIONAL SECURITY WAS CLASSIFIED

We identified information in several documents that was classified for reasons other than national security. The new order prohibits the classification of information unless its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security. The order specifically prohibits classification of information to prevent embarrassment to a person, organization, or agency or to restrain competition.

--A March 1979 message contained a section classified confidential which discussed a commanding officer's plans to host a small function during a visit to a foreign country. Since other sections of the message pertaining to the officer's trip, including the exchange of gifts were unclassified, there did not

appear to be a valid reason for the above section to be classified. The individual who had classified the message agreed that the information should not have been classified. However, he had received informal guidance from his headquarters group that any information on visits by his commander should be classified. This section should not have been classified; it was promptly declassified shortly after the visit was completed.

--A December 1978 message, classified confidential, directed that action not be taken on an earlier, unclassified message which discussed joint support of a defense project at a military installation. The reason for postponing the action was that additional study concerning the project was required. The December 1978 message was originally classified confidential because the classifier believed that the reason for postponing the action could cause embarrassment to his organization. He agreed that the information did not affect national security and should not have been classified and that the message should have been marked "For Official Use Only."

--Estimated funding data for a proposed DOD program was classified confidential in an operational requirement memorandum sent in March 1979. According to the classifier, the information was originally classified because DOD did not want to release estimated funding data for a proposed program. We were told that such data might influence contractors' bids and estimates for a contract. The classifier agreed, however, that such information, if disclosed would probably not damage the national security.

REFERENCES TO CLASSIFIED DOCUMENTS WERE CLASSIFIED

Although both orders state that references to classified documents that do not disclose classified information should not be classified or used as a basis for classification, we identified seven documents that were so classified.

--A January 1979 memorandum was classified because it referred to unidentified submarine photographs. The letter contained no further detail and the classifier agreed that the memorandum should not have been classified. As a result of our discussion in March 1979,

the classifier stated that action would be taken to declassify the letter which was originally scheduled for declassification in January 1985.

--A portion of an April 1979 document was originally classified secret because it mentioned a Defense Intelligence Agency publication that contained secret data. Nothing in the publication was actually discussed and the classifier agreed that the reference to it should not have been classified.

--A March 1979 document had a paragraph classified secret because it mentioned an appendix that was classified secret. Since the title of the appendix was not classified and the paragraph made no reference to any material in the appendix, the classifier agreed that the reference should not have been classified.

THE SAME INFORMATION WAS CLASSIFIED INCONSISTENTLY

One purpose of the implementing instructions to the Executive order is to assure that information relating to national security is protected on a consistent basis. The DOD regulation establishes policies, standards, criteria, and procedures for security classification and requires that these be uniformly applied. However, we identified several instances where the same information was classified at different levels.

--DOD issues a recurring, periodic report to the Congress on the North Atlantic Treaty Organization's (NATO's) defense posture. The report is issued by the Secretary of Defense in three versions--secret, unclassified, and NATO secret. Comparison of the secret and unclassified versions of the January 1979 report revealed identical pages and paragraphs in the unclassified version that were classified in the secret version.

--Two different DOD components originally classified the same type data on force mobility--specific quantities, time, and percentage--at different levels. The classifier in one DOD group originally classified the data as secret. Subsequently, a secret GAO draft report quoted the same type information as part of its analysis. However, when the report was sent to another DOD group for classification and portion marking, it

marked that particular data confidential. The first classifier was unable to explain the inconsistency. He said that he had classified the data secret because, in his opinion, such data is secret. Evidently the second DOD group did not believe the information merited that classification and, therefore, only classified the data as confidential.

--A July 1978 message derivatively classified similar data concerning a particular troop movement in two different parts of the message. The information was classified confidential in one section and secret in the other. The classifier was unable to explain the inconsistency. His supervisor said that the information warranted two different levels of classification because the confidential data referred to U.S. troop movements, while the secret data referred to DOD-imposed troop movements. The words "DOD-imposed" necessitated a higher classification. The supervisor was unable to provide any source material or guidance other than his own feelings to support the different levels of classification.

INFORMATION THAT LOST SOME OF ITS SENSITIVITY WAS NOT DOWNGRADED

The classification level of portions of 16 documents could have been reduced or eliminated because the paraphrasing or summarizing of information in them reduced the sensitivity of the information. Information can be derivatively classified by extracting it verbatim from already classified material or by restating, paraphrasing, or summarizing it from material already classified. Misclassification occurs when (1) the information extracted is not that which made the source paragraph or page classified or (2) the paraphrasing or summarizing reduces or removes the source material's sensitivity and basis for classification.

The new order states that individuals applying derivative markings are responsible for verifying the information's current level of classification as far as practicable before classifying it. They are required to (1) determine if their restating, paraphrasing, or summarizing has removed the basis for classification and (2) classify the document at a lower level, or not at all, when verification with the originator or other appropriate inquiry indicates that a lower level of classification is warranted or that the information should be unclassified. Discussions with individuals who applied

derivative markings and a review of the information they classified, indicated that they were not aware of their responsibility. For example:

--Three documents were classified secret because they had been summarized from secret documents, even though the information had lost much of its sensitivity. The classifiers agreed that the information was less sensitive, but believed that it was their duty to observe the classification levels of source documents.

--In two other instances, classifiers extracted information from source paragraphs marked secret. The classifiers agreed that the information extracted was probably confidential or unclassified, but believed that they were required to follow the classification of source material regardless of their own judgment. No one verified whether the information extracted still had to be classified.

WHEN THERE WAS DOUBT ABOUT THE LEVEL OF CLASSIFICATION, A HIGHER CLASSIFICATION LEVEL WAS ASSIGNED

The new order (as did its predecessor) requires that if there is reasonable doubt as to which level to classify information or whether even to classify the information, the less restrictive classification should be used, or the information should not be classified.

Discussions with classifiers and a review of information that they had classified indicated that this requirement was not always followed. Several classifiers told us that when source material or classification guidance was not clear and they were in doubt as how to classify, they tended to classify at a higher level because the penalties for underclassifying far outweighed those for overclassifying. Discussions with other classifiers indicated that the informal rule of thumb followed was, when in doubt, classify the information at the secret level. The classifiers felt that the confidential level did not provide sufficient protection to the information and that the controls on top secret material made the information too restrictive to deal with. We identified 20 documents that contained one or more examples of information classified at a higher level because the classifiers had doubts about the level of classification.

--Unclassified information was contained in an August 1978 message. Similar information contained in a September 1978 letter was originally classified secret. The classifier pointed out minor differences in the information, but agreed that the letter could have been classified no higher than confidential. He said, however, that when there was a question as to the level of classification, he would rather be safe and use the more restrictive classification.

--One individual classified a portion of a document containing data on war plans as secret, but agreed that the letter should have been confidential. He explained that he had doubts as to the potential damage to national security the disclosure of the data would have caused, and that an informal rule of thumb was to classify all war plans data at no less than the secret level when there is no specific guide requiring another classification.

CONCLUSIONS

Even though the Executive order and implementing instructions clearly describe the types of information that should be classified and even specify other types that should not be classified, our review indicated that a sizable percentage of the information classified was not classified properly. Improper classification causes less information to be made available to the public, reduces public confidence in the system, weakens protection for truly sensitive information, and increases administrative costs.

We believe that the examples described in this chapter demonstrate that a serious problem exists within DOD in that individuals who originally or derivatively classify information either are not fully knowledgeable of the requirements of the order and implementing instructions or prefer to follow a course of action that would result in a lesser penalty to them if they incorrectly classify information.

In our opinion, improved training for individuals classifying information could reduce the incidence of the types of problems discussed above. Such training should emphasize the importance of the requirements of the order and implementing instructions and the responsibilities of each individual who classifies information.

In addition, we believe that the DOD inspection program should direct more attention to evaluating why certain information is classified at a particular level or why it should

be classified at all. These inspections, besides identifying improper classification activity, would instill in the classifiers a greater awareness of the need to exercise maximum care when classifying information to assure that their actions comply with the order and implementing instructions.

Our recommendations concerning improved training and inspections are included in chapter 5.

DOD COMMENTS AND OUR EVALUATION

In commenting on our finding that the classification level of 16 documents could have been reduced or eliminated because the paraphrasing or summarizing of the information in them reduced the information's sensitivity, DOD states that it would be impracticable for individuals to verify all such classification because such procedures would be counterproductive.

We recognize that the Executive order calls for verification when practicable. We also state that the individuals with whom we discussed this matter were not aware of their responsibility. Since the previous Executive order contained a similar provision concerning the responsibility of the individual to verify the classification level when in doubt, we believe that this finding illustrates the need for improved training and education.

CHAPTER 4

CONTINUING DEFICIENCIES IN MARKING CLASSIFIED INFORMATION

The Executive order and implementing instructions clearly specify the markings that are to be shown on each classified document. However, of the 556 documents reviewed, 184, or about 33 percent, were improperly marked in one or more ways. We believe that the incidence of such errors is high, inasmuch as similar markings were required under the previous order and implementing instructions that were in effect from June 1972 through November 1978.

The improper marking of classified information has been a continuing problem for DOD. Even though all components in DOD did not compile and report statistics on improperly marked documents as required under Executive Order 11652, DOD reported about 7,200 such errors in 1977. The report does not indicate how many documents were examined.

At one location visited in March and April 1979, we reviewed five reports of inspections made from October 1976 through October 1978. The marking deficiencies noted during those inspections were similar to those noted during our review. Based on the results of our review, there did not appear to be any significant improvement in the marking process. We identified 31 marking errors on 23 of 31 documents.

Proper marking of classified information is required to provide adequate protection. Properly marked information should preclude its unauthorized or premature disclosure and assure that it is promptly reviewed, downgraded, or declassified. At the time of original classification, documents are required to be clearly marked to indicate

- --the identity of the original classification authority and the office of origin,
- --the date or event for declassification or review or the reason the information is to remain classified for more than 6 years, and
- --the portions of the documents that are classified, with the applicable classification level, and the unclassified portions.

Derivatively classified documents are required to be similarly marked. Noncompliance with these requirements is discussed below.

The following are examples of the marking stamps required by the new order for (1) original classification not in excess of 6 years, (2) original classification in excess of 6 years but not in excess of 20 years, and (3) derivative classification using a guide dated March 1, 1979. The information in the following examples is fictitious, but we have assumed a classification date of June 28, 1979.

Example 1: Classified by Director, Defense Intelligence Agency
Declassify on 28 June 1985

Example 2: Classified by Cdr., 314th Air Division
Review on 28 June 1989
Extended by Commander in Chief, Pacific Air Force
Reason DOD 5200.1, 2-301.6.7

Example 3: Classified by Naval Sea Systems Command Instruction C5511.5
Declassify on 1 March 1985

IDENTITY OF ORIGINAL CLASSIFICATION AUTHORITY AND OFFICE OF ORIGIN NOT SHOWN

Classified documents are marked on the face to show the original classification authority and the office of origin so that questions or challenges regarding the information classified can be directed to the proper sources.

The original classification authority or the office of origin was not shown on 55 of the documents that we reviewed. For example, a March 1979 secret OSD memorandum did not show the classification authority. In addition, it did not contain instructions as to when it was to be declassified and it was not portion marked.

DATE OR EVENT FOR DECLASSIFICATION OR REASON FOR EXTENDED CLASSIFICATION NOT SHOWN

The Executive order requires the classifier to establish a date or event for the declassification or review of the information at the time it is originally classified. This date or event is to be as early as national security permits, in most cases no more than 6 years and no more than 20 years after original classification. Foreign government information may be classified for up to 30 years.

The purpose of specifying a date or event for declassification or review is to ensure that information is declassified as soon as possible. Information that remains unnecessarily classified violates the public's right to know, imposes unnecessary storage costs, and weakens protection for truly sensitive information by undermining respect for all classification.

Also, at the time of original classification, documents containing information classified for more than 6 years are required to be annotated on the face of the document with the reason classification is expected to remain so that any questions regarding the rationale for the prolonged classification are readily explained.

The date or event for declassification or review or the reason for extending classification for more than 6 years was not shown or incorrectly shown on 55 documents.

PORTION MARKING

According to the order, to facilitate excerpting and other uses, each classified document shall, by marking or other means, indicate clearly which portions are classified, with the applicable classification designation, and which portions are not classified. DOD's information security regulation is even more specific in this regard. It states that each section, part, paragraph, subparagraph, or similar portion of a classified document shall be marked to show the level of classification of the information contained in or revealed by it or that it is unclassified. Portions of documents are required to be marked in a manner that eliminates doubt as to which of its portions contains or reveals classified information.

Classified portions not clearly marked

Of the 556 documents, 118, or 21 percent, were not clearly marked to indicate the portions that were classified.

A 50 line paragraph marked secret contained four subparagraphs and covered several pages; however, only three sentences covering eight lines contained classified information. The other 42 lines contained unclassified information. Nevertheless, because the document was not properly portion marked, any of the information on the other 42 lines extracted by someone other than the original classifier would have to be

classified as secret, unless that individual (the derivative classifier) challenged the marking. Thus, information that could be unclassified could remain classified for 6 years or longer.

Portion marking for information classified for more than 6 years

While the order requires that classified documents be portion marked to show the level of classification, it does not require that they be portion marked to identify that part of the information that has to remain classified for more than 6 years. Consequently, classified information that might be declassified sooner, could remain classified as long as the entire document is classified. In addition, if classified documents are subsequently reviewed for declassification, the review process could be facilitated if the documents are marked to identify those portions that required classification for an extended period. Such marking would also facilitate responses to requests made in connection with the Freedom of Information Act.

This potential problem with portion marking takes on added significance because most classified documents are classified for more than 6 years. As noted on page 7, 60 percent of the documents that had a date for declassification or review, were classified for more than 6 years.

One document we identified that illustrates the need for such portion marking was the Office of the Secretary of Defense's Consolidated Guidance. It contained hundreds of pages and provided guidance to all DOD components concerning DOD programs for a 5-year period. According to one official, the Consolidated Guidance for fiscal years 1981-85 was classified for 20 years primarily because it contained intelligence data. It was that official's opinion that much of the information in the volume should not have been classified for that long. However, the entire volume was marked classified for 20 years and, since the information in it that required extended protection was not specifically marked, any of its nonintelligence information derivatively classified by a countless number of individuals in the various DOD components will probably have to remain classified for 20 years.

CONCLUSIONS

DOD has not been able to correct continuing document marking problems. Marking deficiencies noted during our

April 1979 review were similar to those found during DOD's inspections since October 1976.

Marking problems included incomplete or incorrect information stamped on the face of documents and information not adequately portion marked to clearly identify its classification level.

A marking stamp that does not identify who or what office originated the classified information makes it difficult to question or challenge a classification decision if the need should arise. A missing date or event for declassification or review can unnecessarily prolong the classification of information. If the reason information is classified for more than 6 years is not clearly displayed on the face of the document, the user and subsequently the reviewer will not have a clear understanding of why that information requires extended protection.

Further, information that is not adequately portion marked to indicate its classification level can cause unnecessary classification, especially if that information is extracted by someone other than the original classifier, since it is difficult to determine if unclassified material is being extracted from a classified document unless each section clearly specifies which portions are classified and which are not.

In our opinion, improved training of individuals who apply classification markings could reduce the number of marking deficiencies. Our recommendation concerning improved training is included in chapter 5.

Neither the Executive order nor the implementing instructions require portion marking to identify specific portions requiring extended protection to information classified longer than 6 years. The marking on the face of the document only indicates that the entire document requires extended protection. Consequently, information in the document not requiring protection for longer than 6 years could remain classified as long as the entire document is classified. We believe that DOD should require portion marking that identifies the specific information that requires extended protection, especially since DOD is responsible for over 90 percent of the information being classified in Government. However, we recognize that in order to be fully effective, such a recommendation would require Government-wide implementation.

RECOMMENDATION

We recommend that the Secretary of Defense revise the DOD information security program regulation to require that classified documents be portion marked to identify the specific information in them that requires protection for more than 6 years.

DOD COMMENTS AND OUR EVALUATION

While DOD supports the goal of making more information available to the public, it believes that implementation of the above recommendation would require a major and costly program for the periodic review of all documents to identify, separate, reproduce, and provide to the public those portions of classified documents no longer requiring protection. DOD further believes that because of the exchange of classified information among several Federal agencies, the recommendation--even if it was deemed desirable--could not work well in DOD unless it was implemented throughout the executive branch.

It appears that DOD has misinterpreted our finding and recommendation. We are not advocating a special periodic review of classified documents to identify parts thereof that can be declassified sooner than other information in the documents. Our recommendation was primarily directed to derivative classification situations such as the example of the Consolidated Guidance. That is, information not requiring extended classification, that is derivatively classified from originally classified documents, could be identified and so marked and, presumably, declassified at a date earlier than would otherwise be the case. Because of the large volume of information that is derivatively classified in this manner and the fact that most documents are classified for more than 6 years, we believe that our recommendation has merit. Although we agree that the recommendation could not be fully effective without Government-wide implementation, we believe that implementation within DOD would be a good place to start, since DOD accounts for over 90 percent of the information classified by the Government.

CHAPTER 5

IMPROVED TRAINING AND INSPECTIONS NEEDED

As noted in the preceding chapters of this report, serious classification deficiencies persist in DOD. We believe that these deficiencies have continued because (1) individuals who classify information have not had adequate training and (2) formal inspections have not directed sufficient attention to the question of whether information has been properly classified.

INADEQUATE TRAINING OF INDIVIDUALS WHO CLASSIFY INFORMATION

While most of the installations and offices visited had some type of information security education and training program, our discussions with individuals who classify information indicated that such training did not always entail instructions on what information to classify and what classification level to assign. Further, this type of training, when provided, is usually directed to security managers and supervisors who are responsible for developing and implementing security education programs for those who actually classify information within their respective groups. We believe that not providing such training directly to those who classify information was a major cause of many of the classification deficiencies we identified.

Both Executive orders have required agencies to establish training and orientation programs to familiarize employees concerned with classified information with the provisions of the orders and implementing instructions. The DOD information security program regulation requires the heads of DOD components to establish security education programs. According to the regulations, such programs "shall stress the objectives of classifying less information, declassifying more, and improving protection of information that requires it." The program, as a minimum, should be designed to indoctrinate personnel in the principles, criteria, and procedures for the classification, downgrading, declassification, marking, and dissemination of information, as prescribed by the DOD regulation.

In 1974 DOD began offering an information security management course at its Defense Industrial Security Institute in Richmond, Virginia. DOD officials said that the course is the most comprehensive one given in the classification area. It is a 2-week course--1 week focuses on the proper classification of information and the other week covers the physical protection of the information. The

first week addresses the questions of what information to classify, what classification level to assign, and when to downgrade or declassify. In addition to the 2-week course, the Institute offers a condensed 3-day version of the course which is given at the installations that request it.

This course is primarily designed for security managers and other DOD personnel responsible for administering DOD's information security program--to help them develop and implement education and training activities for individuals in their organizations who actually classify information. Through June 1979, the Institute had conducted 43 2-week courses and 45 3-day courses. About 1,900 individuals attended the 2-week courses and about 3,400 participated in the 3-day courses.

In addition to this course the Navy provides its security managers with a security handbook to be used as guidance for developing security education programs for its classifiers. The Navy also has a slide presentation and briefing material which instructs classifiers on what information to classify and at what level.

Army and Air Force officials, however, told us that a comprehensive training program concerning what information to classify, and at what level, does not exist within their departments.

Also, most of the classifiers told us that the security information training and education that they had received generally did not address the actual classification of information. This training generally consisted of orientation briefings for newly hired or transferred staff; periodic security briefings; and memorandums, newsletters, posters, and other security-awareness-type publications. Most of the training concerned the proper marking and safeguarding of information, rather than its proper classification.

At one location we were told that several of the deficiencies that we had identified and brought to the attention of local officials would be discussed in future education efforts.

INSUFFICIENT INSPECTIONS OF THE PROPER CLASSIFICATION OF INFORMATION

Although self-inspections, group or command inspections, and inspector general inspections had been made at each location that we visited, these inspections seldom, if ever,

included an evaluation of whether information had been properly classified. These inspections generally focused on the proper safeguarding of documents, other physical security responsibilities, and proper markings.

Most classifiers indicated that our review was the first time that they had ever been asked by an independent party to justify their classification decisions.

The Executive order requires each agency originating or handling classified information to designate a senior official to conduct an active oversight program to ensure effective implementation of the order. The previous order contained a similar requirement. The implementing instructions issued for both orders make no additional reference to this requirement.

DOD's information security program regulation provides that the head of each military department and component designate a senior official who will be responsible for compliance with and implementation of the DOD regulation. The regulation further provides that such senior officials, within their respective jurisdictions, will be responsible for monitoring, inspecting, and reporting on the status of administration of the program at all levels of activity under their cognizance. There is no requirement or guidance concerning the frequency or the types of inspections that are to be made.

Some groups told us that the day-to-day administrative review that a document receives as it goes through the decisionmaking hierarchy would identify any weaknesses in the classification process; however, based upon the number of errors that we found during our review, it is doubtful that informal, routine reviews of documents eliminate the need for formal, comprehensive inspections for the proper classification of information.

Some individuals also told us that challenges to classification decisions would detect and correct weaknesses in the system, but our discussions with classifiers indicated that formal challenges were rarely, if ever, made. Most classifiers assumed that whoever originally classified the information did so correctly. Several classifiers told us that sometimes they would challenge a classification decision if the classification appeared to limit distribution or seriously inhibit working with the document.

While the challenging process could be beneficial to the program if fully implemented, it should not be considered a substitute for formal inspections that review classification decisions. Most security managers and classifiers told us that they believed that more formal and comprehensive inspections would be helpful to the program. Officials from one organization told us that inspections that covered classification decisions were needed and would be instituted at that organization.

CONCLUSIONS

We believe that DOD's information security training program should direct more attention to the individuals who actually classify information. Such training should include detailed instructions on who can classify national security information and how to properly classify and mark it.

Additional training should contribute to a reduction in improper use of classification authority, improper classification of information, and improper marking.

While the areas covered by the various DOD inspections--physical safeguards and markings--are important, we believe that the propriety of the classification decisions is equally important. These inspections, as a minimum, should include a determination of whether information should be classified and, if classified, whether it is classified at the proper level.

RECOMMENDATIONS

We recommend that the Secretary of Defense revise the information security program regulation to provide for expanded training for individuals who classify information, originally or on a derivative basis, and that such training among other things, should concentrate on

--the responsibility of all individuals to comply with the Executive order and implementing instructions,

--who can classify national security information,

--what information is to be classified, and

--how to properly classify and mark such information.

We further recommend that the Secretary of Defense revise the information security program regulation to provide definitive guidance on the frequency of the different levels

of inspections that should be made and the items to be covered by such inspections, with special reference to the need for inspections to question the propriety of classification decisions.

DOD COMMENTS AND OUR EVALUATION

DOD believes that the discrepancies noted and presented in this report "do not convey nor support a premise of noncompliance with the requirements of Executive Order 12065," but that they do underscore the continuing need for senior-level awareness of the program and management support for education and training efforts. As indicated by our recommendation, there is a need for more education and training. Moreover, that recommendation was based upon a large number of examples of noncompliance with the Executive order and implementing regulations and instructions.

DOD further believes that the errors identified "were generally minor in nature" and found in documents classified within 6 months or so of the effective date of the new order and occurred because many individuals were still unfamiliar with the new security classification system. We believe that DOD is incorrect in categorizing many of the errors as "minor in nature." For instance, 24 percent of the documents we reviewed contained one or more examples of improper classification of national security information. In our opinion, examples such as these could hardly be considered minor. We also believe that DOD's assertion that the errors were caused by unfamiliarity with the new order is incorrect because most of the provisions of the new order--with which deficiencies are identified in this report--are identical or similar to provisions of the previous order which had been in effect since 1972.

DOD believes that the provisions of the information security program regulation pertaining to training are adequate, but that it is considering ways to improve its "already good security education and training programs." We believe that the examples cited in this report illustrate the need for improvement in those programs and that including certain basic points for such programs in the regulation would direct attention to them. We further believe that the establishment of minimum training standards that would increase the number of individuals who receive such training is vital if DOD is to improve implementation of its classification program.

With respect to our recommendation concerning the frequency and types of inspections to be made, DOD states that our use of the term "different levels of inspections" is unclear and that the necessity for inspections is basically a command function and will vary greatly between units. Nevertheless, DOD says that it will consider the basic concept of our recommendation--to provide guidance on the minimum frequency of security inspections and areas to be covered. Although our recommendation did not specify the different levels of inspections, they are identified on page 26 as self-inspections, group or command inspections, and inspector general inspections.

APPENDIX I

POLICY

THE UNDER SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

5 OCT 1979
In reply refer to:
I-09445/79

Mr. R. W. Gutmann
Director, Logistics and Communications Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Gutmann:

This is in response to your draft Report to the Congress (OSD Case No. 5268) (Code 941180), "Continuing Problems in DoD's Classification of National Security Information" that was forwarded to the Secretary of Defense by your letter of August 27, 1979 wherein you invited comments regarding the draft Report.

The discrepancies noted and as presented in the draft Report do not convey nor support a premise of noncompliance with the requirements of Executive Order 12065, "National Security Information." They do underscore the continuing need for senior level awareness of the Information Security Program and management support for education and training efforts.

The Department's views concerning the draft Report are set out in the attachment.

Sincerely,

Ronald H. Stivers

for Daniel J. Murphy
Admiral, USN (Ret.)
Deputy

Attachment

APPENDIX I

DEPARTMENT OF DEFENSE COMMENTS
CONCERNING UNITED STATES GENERAL ACCOUNTING OFFICE
DRAFT REPORT TO THE CONGRESS DATED AUG. 27, 1979
(OSD CASE NO. 5268) (CODE 941180)

The third full paragraph on page 3 of the draft Report indicates that 49 percent of the 556 classified documents reviewed by the GAO were found to have at least one of many possible errors. A review of the report indicates those errors were generally minor in nature and found in documents classified within a half year or so of the effective date of Executive Order 12065, a period of time during which the Order's new security classification system was still unfamiliar to many people. As experience with the new system is gained, it is expected that the error rate will diminish.

The second paragraph on page 4 of the draft Report indicates the GAO review of classified documents was hampered by the refusal of the Office of the Joint Chiefs of Staff (OJCS) and the Air Force to make certain documents available. The documents requested in the OJCS instance were Joint Strategic Planning System (JSPS) documents. In response to the request, the GAO team leader was informed, by memorandum, that access to such documents is severely limited because of their sensitivity and that the GAO requirement for such documents for the purpose of conducting a security classification review was not evident. The documents that had been requested at the Air Force were originated by the JCS and Defense Intelligence Agency or in response to those organizations. The distribution limitations reflected in the documents were imposed by those organizations to preclude release by other than the JCS or DIA. It is our view that the effectiveness of the GAO survey was not diminished by these restrictions. This is evidenced by the conclusions and recommendations in the draft report which were based on inspections of a wide variety of other classified material.

On pages 6 and 7 of the draft there is a discussion of an incident involving the unauthorized use of the position title of an original Top Secret classification authority by personnel of a command who were authorized to originally classify information at the Secret or Confidential levels. The draft points out that the memorandum granting that authority was rescinded and replaced by a security classification guide that only sets the minimum level of classification and the maximum duration of classification for the categories of information identified by the guide. The Department's Director of Information Security has since requested (by memorandum of 13 July 1979) that a number of changes to the guide be made to overcome its weaknesses.

The paragraph that begins on page 7 and continues on page 8 of the draft Report indicates that a DoD organization specified in writing 17 items of information that should be classified longer than six years. Presuming that the correspondence was approved by the commanding officer of the organization, the only person with original Top Secret classification authority in the organization, and that the list identified specific items of information to be classified for stated periods of time in excess of six years, the correspondence was in effect a security classification guide within the meaning of the Executive Order.

On page 10 of the draft there is a RECOMMENDATION "that the Secretary of Defense revise the information security program regulation to require that all classification guides and revisions thereto be reviewed by an official other than the originators of the guides, to assure compliance with the provisions and intent of the executive order and the DoD regulation. We further recommend that deviations from the requirements of the executive order or the regulation, noted during these independent reviews, be brought to the attention of the Director of Information Security to assure their prompt resolution."

It is understood that the foregoing recommendation is undergoing minor revision. In any event, review of classification guides by other than the originator is already common practice within the Department though not specifically required as such by the Regulation. With modification, the Department will consider the second part of the recommendation. Referral of deviations from the Order and Regulation to the Director of Information Security would be appropriate only in those cases of unresolved problems within or between DoD Components.

The second paragraph on page 15 of the draft Report contains a statement to the effect that "the classification level of 16 documents could have been reduced or eliminated because the paraphrasing or summarizing of information in them reduced the sensitivity of the information." An individual using source documents from other agencies must respect the original classification determination of those agencies. If in doubt, and when it is possible, that individual should verify the classification, but one cannot practically verify every classification decision or submit every paraphrase to the originating agency for a classification determination. Such procedures would prove counterproductive.

There is a RECOMMENDATION on page 24 of the draft that states "We recommend that the Secretary of Defense revise the DoD information security program regulation to require that classified documents be portion marked to identify the specific information in them that requires protection for more than 6 years."

The Department of Defense must nonconcur with the foregoing recommendation. The draft Report indicates that such markings as recommended would make more information available to the public at an earlier date. The Department supports the goal of making more information available sooner, but to be effective in this context, the GAO recommendation would require a major and costly program for the periodic review of all documents to identify, separate, reproduce, and provide to the public those portions of classified documents no longer requiring protection in the interests of national security. The product of such an effort would be a disjointed accumulation of bits of the whole story on a given subject that would be of little value to the public and may even be misleading. Further, the recommended marking scheme may not actually facilitate reviews for declassification such as those done under the Freedom of Information Act. Such a review for declassification must be based on a reevaluation of the continuing sensitivity of the information. Marking portions with a duration of classification might lead to an unacceptable "automatic" review where the reviewer might tend to accept as still valid the original classifier's judgment as to which portions of a document require extended classification. As the draft notes, this recommendation goes beyond the requirements of the Executive Order and its implementers. It could not work well in this Department alone even if it was deemed to be desirable. Executive Branch-wide implementation of the recommendation would be required due to the exchange of classified information among the several departments and agencies.

On page 28 of the draft there is a RECOMMENDATION that "the Secretary of Defense revise the information security program regulation to provide for expanded training for individuals who classify information, originally or on a derivative basis, and that such training, among other things should concentrate on

-- the responsibility of all individuals to comply with the executive order and implementing instructions,

-- who can classify national security information,

-- what information is to be classified, and

-- how to properly classify and mark such information."

The Department is considering ways to improve its already good security education and training programs. That action would be ongoing even in the absence of the foregoing recommendation that is based on a review of a very small sample of classified documents - half of which had minor errors. It is believed that the provisions of the Regulation are adequate.

APPENDIX I

There is a second RECOMMENDATION on page 28 of the draft stating that "We further recommend that the Secretary of Defense revise the information security program regulation to provide definite guidance on the frequency of the different levels of inspection that should be made and the items to be covered by such inspections, with special reference to the need for inspections to question the propriety of classification decisions."

With respect to the foregoing, the use of the term "different levels of inspection" is unclear. It should be recognized that inspection for compliance with DoD or Component requirements of all kinds is basically a function of command and that the necessity for inspection for compliance with the Information Security Program Regulation will vary greatly between units or elements at the same level of subordination. Notwithstanding, the Department will consider the basic concept of the recommendation, i.e., to provide guidance on the minimum frequency of security inspections and areas to be covered.

GAO Note: Page references in this appendix have been changed to agree with the page numbers in the final report.

(941180)

AN EQUAL OPPORTUNITY EMPLOYER

UNITED STATES
GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE,$300

POSTAGE AND FEES PAID
U. S. GENERAL ACCOUNTING OFFICE

THIRD CLASS