[redacted]

STATEMENT OF J. FRED BUZHARDT

GENERAL COUNSEL OF THE DEPARTMENT OF DEFEN

TO THE

SUBCOMMITTEE ON INTELLIGENCE

OF THE

HOUSE ARMED SERVICES COMMITTEE

MARCH 8, 1972

Mr. Chairman, Distinguished Members of the Subcommittee:

The Department of Defense welcomes this opportunity to discuss the security classification and declassification system as it applies to national security information and material and to acquaint this Subcommittee with the practical operating problems associated therewith.

Accompanying me this morning is Mr. David O. Cooke, Deputy Assistant Secretary (Administration).

Major Changes in the Executive Order

The President has just issued a new Executive Order on Classification and Declassification of National Security Information and Material to be effective on June 1, 1972. It replaces Executive Order 10501, which, although amended several times, has governed the security classification program since it was issued in 1953.

The new Executive Order departs from its predecessor Order in a number of respects. The changes are based on the lessons learned under Executive Order 10501. The most significant changes are the constraints on initial classification and the changes in downgrading and declassification. The principle changes are as follows:

(1) The number of Departments and Agencies authorized to classify at any given level of classification is reduced;

(2) The authority of the heads of Departments and Agencies to delegate classification authority within each Department or Agency is more restricted;

(3) The class of persons to whom authority to declassify can be delegated is specifically not limited to those who are eligible for a delegation of authority to classify;

(4) The downgrading and declassification schedule is accelerated;

(5) Exceptions to the general downgrading and declassification schedule are limited to four specific categories of information;

(6) All classified information which is not automatically declassified at the end of 10 years is made subject to a mandatory classification review upon request;

(7) All classified information not sooner declassified is automatically declassified at the end of 30 years unless the head of the Department personally determines in writing at the time to continue protection for specified reasons;

(8) Information classified under previous executive orders and more than 30 years old is to be systematically reviewed and declassified by the Archivist;

(9) A mechanism is established to review departmental and agency implementation of the system, and to consider and take action on complaints;

(10) Administrative reprimands are authorized for employees who overclassify information in flagrant cases; and

(11) The definitions of information which qualifies for classification in each category is reworded in terms of "national security" rather than "national defense."

These and the other changes made in the Executive Order resulted from the President's decision to limit the quantity of material to be classified and the time it remains classified while providing more protection to that which is classified.

Before summarizing the new Executive Order in more detail, I will comment on the authority for the Executive Order.

Authority for the Executive Order

The President's authority to issue Executive Orders is derived from Article II of the Constitution. Section 1 of Article II provides that the Executive power shall be vested in the President of the United States. Section 2 provides that the President shall be Commander in Chief of the Armed Forces. Section 3 provides that he shall execute the laws.

The President's authority to restrict the dissemination of information is expressly recognized by various statutes. For example, 18 U.S. Code 793 refers to information which the President has determined would be prejudicial to the national defense. 18 U.S. Code 795 makes it a criminal offense to photograph or graphically portray any military installations or equipment defined by the President as "requiring protection against the general dissemination of information relative thereto." 18 U.S. Code 798 refers to classified information which is specifically designated for restricted dissemination for reasons of national security. 50 U.S. Code 783 refers to information which has been classified by or with the approval of the President, because it affects the security of the United States.

Perhaps the clearest Congressional acknowledgement of the President's authority to restrict the dissemination of information is found in 5 U.S. Code 552, sometimes referred to as the Freedom of

Information Act. Section 552 directs each agency to make available to the public stated categories of information. However, Subsection (b) thereof provides that the act shall not apply to matters that are "specifically required by executive order to be kept secret in the interest of national defense or foreign policy."

The Supreme Court has also acknowledged the President's power of classification. For example, the authority of the President in this area is recognized in the concurring opinion of Justice Stewart in New York Times v. United States and United States v. Washington Post Company et al, 91 S. Ct. 2140 (1971). In Justice Stewart's words, "*** it is clear to me that it is the constitutional duty of the Executive -- as a matter of sovereign prerogative and not as a matter of law as the courts know law -- through the promulgation and enforcement of Executive regulations, to protect the confidentiality necessary to carry out its responsibilities in the fields of international relations and national defense."

In his separate concurring opinion, Justice Marshall declared, "In this case, there is no problem concerning the President's power to classify information as 'Secret' or 'Top Secret'. Congress has specifically recognized Presidential authority which has been formally exercised in Executive Order 10501 to classify documents and information."

Chief Justice Burger, in his dissenting opinion, also readily acknowledged the inherent power of the Chief Executive to classify papers, records and documents as secret.

In considering the President's power to designate information as subject to restricted dissemination, the distinctions between classified information, Congressional access, and Executive Privilege must be kept in mind.

First, information which is classified because its unauthorized disclosure could damage national security is not the only category of information the dissemination of which is lawfully restricted by the Government.

Second, the fact that information is classified is not determinative of the right of access by the Congress to the information.

Third, the doctrine of Executive Privilege by which the President may decline to disclose information to the courts or to Congress is separate and independent from the power to classify, and neither power is contingent upon the other.

Development of the New Executive Order

The new Order is a result of an in-depth review of the security classification and safeguarding procedures in the Executive Branch. In January 1971, at the direction of the President, a National

Security Council memorandum directed a comprehensive study of Executive Order 10501. On March 2, 1971, an Ad Hoc Group met to prepare responses to specific questions contained in the National Security Council memorandum. The Ad Hoc Group was chaired by an Assistant Attorney General and was comprised of representatives from the Departments of Defense and State, the Central Intelligence Agency, the Atomic Energy Commission and the National Security Council.

In the succeeding months, the Ad Hoc Group prepared a series of recommendations and a draft Executive Order. Subsequently, each of the concerned Departments and Agencies reviewed the draft proposal exhaustively and provided detailed comments and suggestions. Consequently, the whole spectrum of factors bearing on the subject matter, as well as a wide variety of viewpoints, were available to the President and his staff as the new Executive Order was drafted.

The Executive Order

At this point, I would like to provide a somewhat more detailed comment on the new Executive Order and the reasons which underlie its provisions.

(1) Classification criteria and categories.

Classified information is defined in terms of whether the information, if disclosed to unauthorized persons, could reasonably

be expected to cause damage to the national security. The term "national security," as used in the Executive Order, includes both national defense and foreign relations matters. The use of the term "national security," rather than "national defense," recognizes that the category of information requiring protection is broader than military information alone, and is also more consistent with the provisions of the Freedom of Information Act (5 U.S.C. 552) which exempts from public disclosure matters that are "specifically required by Executive Order to be kept secret in the interest of the national defense or foreign policy."

The three categories of classified information - Top Secret, Secret and Confidential - prescribed in Executive Order 10501 are retained in the new Executive Order. The distinctions among the three categories still turn on the degrees of damage to national security that could result from failure to protect the information from disclosure.

Some criticism of the multiple categories of classification has been made. Whatever advantages might result from a single classification category are far outweighed by the adverse consequencies. Historically, the degree of protection afforded to classified information has been dependent upon the degree of damage to the national security involved in the risk of disclosure. The reasons for varying the degree of protection afforded are also practical ones. Each element of protection

afforded classified information involves monetary costs and some administrative encumbrances.

For example, I am informed that the type of investigation required for a security clearance at a confidential level -- a National Agency Check -- costs on the average $5.44 per investigation; but the full field background investigation which is required for a security clearance at the Top Secret level costs an average of $263.28 per investigation.

If there were but one category of classified information, it would be necessary to conduct the equivalent of the investigation now required for a Top Secret security clearance for all personnel cleared at any level of classification in order to afford the highest protection to material within the category. Based on the number of security clearances presently outstanding, it is estimated that the one time dollar impact would be in the neighborhood of an estimated $828 million and the annual costs of background investigations would rise from $53 million to the vicinity of some $500 million.

There are also substantial costs associated with the handling, transportation and storage of classified information and material both within the Federal Government and in private industry. These costs also vary according to the degree of protection provided and, consequently, with the level of classification.

Providing a high degree of protection, such as is now afforded to Top Secret information and material, also has an inhibiting effect on administrative and operational flexibility. If there were but one category of classified information -- which would mean that all classified information and material would be provided that same high degree of protection -- the efficiency of operations and administration by those having to deal with classified material would be seriously impaired.

There is an additional consideration which stems from the necessity of synchronizing our classification system with those of our NATO Allies. More than two decades of negotiations have resulted in the acceptance by NATO of multiple classification categories. If the United States classification system were now abandoned in favor of a single classification category, the resulting confusion in dealing with NATO would be considerable.

(2) Authority to classify.

Under Executive Order 10501, 38 Departments and Agencies had the authority to classify at the Top Secret level which is inclusive of authority to classify at the Secret and Confidential level. Under the new Executive Order, only 12 Departments and Agencies aside from the offices of the Executive Office of the President are authorized to classify information at the Top Secret level. An additional 13 Agencies are

delegated the authority under the new Executive Order to classify information at the Secret level.

The new Executive Order provides authority to delegate within a Department or Agency only to a limited number of officials. Top Secret classification authority may not be delegated below the level of the principal Deputies or Assistants of major elements of the Department or Agency. In the 13 Agencies authorized to originally classify information Secret, classification authority may not be delegated below the senior principal Deputies or Assistants to the head of the Agency. Under Executive Order 10501, classification authority at the Top Secret level can be delegated to any person employed by the Department or Agency.

The constraints on the classification authority imposed by the new Executive Order represent the most severe limitations on that authority which are practical. To limit further the numbers of persons authorized to classify would constitute an impairment of the objective for which the system is designed. Information which, if disclosed, could damage the national security, can originate or come into the possession of the Government at a wide variety of locations and at all levels of Government and associated industry: the drawing board, the laboratory, the test range, in an Embassy or on an Army squad patrol. To protect adequately such information, someone with authority to classify

must be available near the official source if the information is to be adequately protected in transmittal to the ultimate user. Considered in the light of such practical considerations, the provisions of the new Executive Order limiting the proliferation of classification authority go as far as possible without impairing the effective operation of the classification system.

(3) Authority to downgrade and declassify.

Under Executive Order 10501, the authority to downgrade and declassify accompanied the authority to classify. No individual could be delegated the authority to downgrade or declassify who was not delegated the authority to classify. Under the new Executive Order the authorization to heads of Departments or Agencies to delegate downgrading and declassification authority is not so limited. In addition to those persons within the Department or Agency to whom are delegated the authority to classify, the head of the Department or Agency may delegate to others also the authority to downgrade and declassify.

In practical effect, this has the potential for significantly increasing the capability of Executive Departments and Agencies to review and declassify information and materials more rapidly and efficiently. The new Executive Order reflects a recognition that the senior officials authorized to classify are usually the busiest and

consequently they have insufficient time to adequately review, downgrade and declassify information for which protection is no longer justified. Under the new Executive Order, it will be possible for the heads of Departments and Agencies to designate specific individuals who are not preoccupied with other functional responsibilities to review, downgrade and declassify such information.

(4) Rules for classification.

The Executive Order just issued establishes a new guiding principle -- each person possessing classification authority shall be held accountable for the propriety of his or her classifications actions.

To enable enforcement of this principle, the new Executive Order provides that information and material classified under the Order shall indicate on its face, or on a separate record, the identity of the individual authorizing the classification.

(5) Rules for downgrading and declassification.

Under Executive Order 10501, all information classified at the Top Secret, Secret or Confidential level is also required to be grouped into one of four categories for purposes of downgrading and declassification.

Group 1 information and material is excluded from automatic downgrading and declassification. It consists of information or material originating with foreign governments or international organizations,

information and materials protected by statute, such as that falling within the purview of the Atomic Energy Act, and information or materials requiring special handling, such as intelligence or cryptology.

Group 2 information or material is also exempt from automatic downgrading and declassification. It consists of extremely sensitive information or material which the head of the Agency or his designee designates.

Group 3 information or material is exempt from automatic declassification, but is subject to automatic downgrading at 12-year intervals until it reaches the lowest classification. It consists of that information or material which warrants some degree of classification for an indefinite period.

Group 4 includes all classified information or material not falling in Groups 1, 2 or 3 and is subject to downgrading at 3-year intervals and automatic declassification 12 years after the date of original issuance.

Under the new Executive Order, separate groupings for purposes of downgrading and declassification are dispensed with. In lieu of the grouping system, a General Declassification Schedule is prescribed, to which limited exceptions are specified and subjected to special rules for downgrading and declassification.

follows: Top Secret information is automatically downgraded to Secret at the end of 2 years from the date of original classification; further downgraded to Confidential at the end of 4 years from date of original classification; and is declassified at the end of 10 years from the date it was originated.

Secret information is automatically downgraded to Confidential at the end of 2 years and automatically declassified at the end of 8 years from the date it was originated.

Confidential information is automatically declassified at the end of 6 years from the date it was originated.

This provides for an automatic downgrading and declassification schedule at intervals of 2 years, 4 years and 10 years as compared to the most rapid downgrading and declassification under the old system -- that applicable to Group 4 -- at intervals of 3 years, 6 years and 12 years from original date of classification.

Four limited and specific categories of information are authorized to be exempted from the General Declassification Schedule specified in the new Executive Order. The specific exemption category must be specified in writing on the document or material. The four exemptions cover information or material which fall into one of the four following categories:

A. Classified information or material furnished by foreign governments or international organizations and held

by the United States on the understanding that it be kept in confidence.

B. Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.

C. Classified information or material disclosing a project, plan, installation or system or a specific foreign relations matter the continuing protection of which is essential to the national security.

D. Classified information or material the disclosure of which would place a person in immediate jeopardy.

Information or material falling into one of the categories eligible for exemption may thus escape automatic downgrading and declassification. However, such material is made subject to a mandatory classification review any time after the expiration of 10 years from date of origin upon request by a Department or a member of the public.

In addition to the mandatory review upon request at the end of 10 years, the new Executive Order provides for automatic declassification at the end of 30 years from origination of all classified information unless the head of the originating Department personally determines in writing at the end of 30 years that continuing protection is essential

to the national security or that its disclosure would place a person in immediate jeopardy. Under the provisions of Executive Order 10501, classified information falling in Groups 1, 2 and 3 was subject to no automatic declassification.

The Executive Order provides that information classified before the effective date of the new Order, regardless of the Group to which it was assigned, shall be subject to mandatory review at the end of 10 years from origination in accordance with the rules which apply to the mandatory review for information or material exempted from the General Declassification Schedule under the new Order. Similarly, all information and material classified before the effective date of the new Order which is 30 years or more old shall be systematically reviewed for declassification by the Archivist of the United States.

These new rules for downgrading and declassification constitute the most significant and far reaching changes in the classification system and the Executive Order which governs it. They are designed to insure a more rapid and more comprehensive flow of previously classified information to the public.

(6) Implementation and review mechanisms.

The new Executive Order provides that each Department or Agency originating or handling classified information shall form a

Departmental committee to act on all suggestions and complaints with respect to the Department's administration of the Order.

Even more important, however, the Order establishes an Interagency Classification Review Committee under the National Security Council. This Committee is to be composed of representatives of the Departments of State, Defense and Justice, the Atomic Energy Commission, the Central Intelligence Agency, and the National Security Council staff. The Chairman is to be designated by the President.

The Interagency Classification Review Committee has the following responsibilities:

A. To monitor Department actions to insure compliance with the provisions of the Executive Order and such implementing directives as are promulgated by the National Security Council;

B. To receive, consider and take action on suggestions and complaints from persons within or outside the Government on the administration of the Executive Order; and

C. In consultation with the affected Department or Departments, to assure that appropriate action is taken on suggestions and complaints.

The Executive Order requires Departments and Agencies to furnish the Committee any particular information or material needed by the Committee to carry out its functions.

The Interagency Classification Review Committee is an innovation in the new Executive Order. It provides for the first time a continuing mechanism to examine the effectiveness and the implementation of the Executive Order, and makes it possible to address one of the most fundamental problems in any classification system; that is, assuring that decisions to classify or not to classify are responsible and objective.

The consequences of improper classification decisions are serious, regardless of the direction of the error. If information or material, the disclosure of which would not damage the national security, is classified, a series of adverse consequences flow. The public is denied information to which it has a right, and the credibility of the entire classification system is damaged. Unnecessary classification requires unnecessary restrictions on the flow of information within the Government as well as outside, and the flexibility and efficiency of the Government's work is diminished. Providing security in handling, storage and communication of the classified material is expensive and, consequently, unnecessary classification wastes resources.

On the other hand, failure to classify and to protect information, the disclosure of which could damage the national security, can obviously result in a spectrum of adverse effects, ranging from the loss of lives to jeopardizing the very existence of the Nation.

Despite the potential for dire consequences which can result from erroneous decisions on questions of classification, individual judgments must unavoidably remain at the heart of the classification system. Criteria for classification must be and are imposed, but due to the variety and complexity of the types of information which must be considered for classification, there must remain flexibility for the exercise of individual judgment.

The review procedures initiated in the new Executive Order provide a means to insure an increased measure of care and consistency in the decisions on classification. The potential for review and action on complaints, coupled with the identification of the classifier and the authorization for administrative reprimands of those who abuse classification authority should combine to reduce substantially, if not eliminate, casual or indifferent classification actions.

(7) Special provisions.

There are several special provisions in the new Executive Order which are worthy of particular note.

In the past, declassification authority has resided with the originating Department or Agency. This posed special problems with

regard to information classified personally by a President, his White House staff, or any special committee or commission appointed by him and given classification authority.

For the most part, information so classified is deposited with the Archivist of the United States when a President leaves office. In the past, there has been no specific provision as to who had the authority to declassify such documents.

The new Executive Order places that authority in the Archivist of the United States, subject to the donor's deed of gift, consultations with Department having a primary interest in the subject matter, and subject to the provisions of the Executive Order relating to declassification.

The new Executive Order also contains special provisions for the granting of access to classified information or material for the purpose of historical research projects and, in limited cases, to former Government officials.

Operational Problems

I will turn now from the Executive Order and touch on some of the more difficult operational problems associated with or related to the security classification system.

(1) Controlling the number of security clearances.

Closely allied with the security classification system are the various personnel security programs which cover civilian employees of the Department, members of the Armed Forces, and contractors and their employees who work on classified materials or require access to classified information in the performance of Government contracts. The security clearance program of civilian employees and of participants in the industry security program are covered by separate Executive Orders. The security clearance program for military personnel is established by a Department of Defense directive.

Under the foregoing programs, there are an estimated 3.6 million security clearances in all categories now outstanding. Of these, only 464,550 are Top Secret clearances. This 464,550, incidentially, represents a reduction by 31.2 percent since mid-1971, at which point in time there were more than 697,000 clearances outstanding. The decrease resulted from a concentrated reduction program directed by the President.

There is a constant need and requirement to control and keep at a minimum the number of security clearances outstanding both for the purpose of saving money and for the purpose of providing better protection to classified information and materials. The biggest payoffs are obviously

in the control of clearances at the Top Secret level both in terms of cost and protection.

At this point, I digress to point out that the numbers of persons holding security clearances alone are not a reliable indicator of the number of persons having access to highly classified information. Although a security clearance is a prerequisite to access to classified information, only those who also have a "need to know" are authorized access and then only to the extent that their official duties require it. Possession of even a Top Secret clearance does not indicate that the possessor necessarily has, or was ever intended to have, access to Top Secret or even classified information or documents. The security clearance may be required for duties involving classified materials, as distinguished from information or documents. For example, security guards on some types of installations hold Top Secret clearances but rarely, if ever, have a "need to know" Top Secret or Secret informatio

ILLEGIB

Of the approximately 3.6 million clearances in all categories approximately 1,266,000 are outstanding in the industrial security program. By far the overwhelming proportion of these are at the Secret and Confidential level. The numbers, to a large extent, reflect the numbers of technical and production workers engaged in performing contractual work on classified products for the Department of Defense.

Similarly, of the approximately 3.6 million clearances in all categories, approximately 1.6 million are issued to military personnel. Again, a very large proportion of the number of those clearances are attributable not to a need for access to classified information, but rather for access to classified material in order to operate, maintain, handle or process classified military hardware.

From this, it is apparent that in terms of all clearances outstanding in all categories, the most significant determinants are the numbers of industrial personnel working on classified products for the Department of Defense, and the number of military personnel who must be associated with classified weapons and other hardware.

When these factors are taken into consideration, it becomes more apparent that the number of clearances at the Top Secret level is the most fruitful area for efforts at reduction of numbers, and that an approximately 1/3 reduction in the number of such clearances in recent months represents very significant progress.

(2) Controlling the volume of classified documents.

There is also a problem associated with controlling the volume of classified documents required to be stored. The excesses in this connection largely result from time pressures which prevent the review, declassification or destruction of classified documents which

are no longer needed. It is difficult to devise a means within the resources available to assure that numerous offices are not retaining and storing copies of identical classified documents which are no longer needed for current operation or administration.

Former Deputy Secretary of Defense David Packard adopted a simple, but novel, remedy. He declared a moratorium on the acquisition of additional security containers by Department of Defense elements. This moratorium, still in effect, at least limits the accumulation of any larger volume of classified documents.

(3) Controlling costs of Background Investigations.

As I noted earlier, the current average cost of a full-field or background investigation is $263.28 per investigation. Because of the significant cost, it is incumbent on the Department to limit such investigations to only those which are essential, and to conduct those which are necessary with maximum efficiency and effectiveness. In the past, each Military Department has conducted background investigations for their own military members, civilian employees and the industrial employees of contractors of the particular military service. Full-field investigations necessitate inquiries in all geographical areas of the country. Each Service, therefore, has found it necessary to maintain field offices in various locations throughout the country.

In addition, among Military Departments there have existed variances in methods and approaches for background investigations, which condition has in some cases inhibited the acceptance by one military department of a full-field investigation conducted by another.

From this general description, it is apparent that the system used in the past was susceptible to some duplication of effort and to varying levels of efficiency, both from the standpoint of time required to conduct and process an investigation, and its average costs.

On November 5, 1971, the President directed that a Defense Investigative Service be created to conduct personnel security investigations for all Department of Defense and affiliated personnel. On December 29, 1971, the Secretary of Defense implemented the President's order by directing the establishment of the Defense Investigative Service which combines the personnel security investigative resources of the three military departments into a single agency. The Defense Investigative Service will begin operation on April 1, 1972, by taking operational control of the personnel security investigative resources now operated by the military departments. Subsequently, these resources will be transferred on a time-phased schedule to the Defense Investigative Service. Last week, the Secretary of Defense appointed Brigadier General J. J. Cappucci, formerly the

Director of the Air Force Office of Special Investigations, as the Director of the Defense Investigative Service.

This consolidation of investigative resources centralizes responsibility and is expected to result in substantial long-run savings, as well as increased efficiency.

(4) Problems connected with unauthorized disclosures of classified information.

There are a number of problems which arise in connection with unauthorized disclosures of classified information which are deserving of comment.

In general, disclosures which appear to contravene the provisions of the Federal Criminal Code generally fall within the investigative jurisdiction of the Department of Justice. The Department having a primary interest in the disclosure cooperates with the investigation, and the degree of participation by the Department depends largely on the nature of the disclosure.

In other types of security violations, investigations are conducted by the Department. For instance, if the disclosure results from carelessness, such as leaving a classified document on the desk overnight, the likelihood of disclosure to a potential enemy is not as great, and the inquiry is normally conducted by Department of Defense personnel. In

practice, a crucial judgment must often be made on the question of whether a formal investigation should be initiated in connection with a particular disclosure. The conduct of a formal investigation, if disclosed, as it usually necessarily is, can have the affect of authenticating that the information disclosed is at least partially accurate and that the disclosure is considered to be of serious proportions. If, for example, a news or opinion article in the media contains some elements of accurate, classified information interspersed with speculation and some inaccuracies, less damage to the national security may result from leaving the reader, and possibly even the writer, to speculate on which, if any, of the material is accurate than to risk authenticating the disclosure by the act of conducting an official investigation. If, however, there are indications that the compromise or disclosure may have espionage implications, an investigation is essential in order to terminate the source of the compromise or disclosure.

We in the Department of Defense are not interested in investigating newsmen or newswomen, but we do have a responsibility to investigate instances where Defense personnel are involved in unauthorized disclosures.

Even when by investigation the source of the compromise or disclosure is determined, the question of whether to prosecute often remains a serious one. Among the considerations is again the question

of authentication of the material compromised. It is also sometimes necessary for the purposes of prosecution that classified material be declassified for use in the trial. At this point, a decision maker within the Department must make a judgment as to whether any additional damage to the national security which might result from the declassification is outweighed by the prospects for a successful prosecution.

The requirement for declassification of material is by no means the only risk of damage to the national security which can arise from a decision to prosecute in cases of unauthorized disclosure. In some cases, there may be a disclosure of an amount of classified information which is quite limited and of low sensitivity compared to the total amount of classified information known to the person who made the disclosure and who is the prospective defendant. Depending on the personality, apparent motive for the prior disclosure, mental condition and even power of recall of the person who made the unauthorized disclosure, the risk to the national security from further disclosures by the defendant during the trial could outweigh the advantages of prosecution.

Obviously, under these and similar circumstances, prosecution cannot and does not result from every successful investigation of an unauthorized disclosure which is prohibited by the Criminal Code. In all cases, regardless of whether prosecution occurs, every effort is made to prevent further disclosures.

Comments on H. R. 9853

Mr. Chairman, I have this morning provided to the Committee the views of the Department of Defense on H. R. 9853, "To amend the National Security Act of 1947 to provide for a continuing review and study of measures that should be taken with respect to the designation and protection of information within the Department of Defense and certain other agencies which affects the national security."

The Department of Defense recommends that no action be taken on H. R. 9853.

As I have noted earlier in my statement, the security classification program has been the subject of study and review by an Ad Hoc Interagency Group over the immediately preceding period of more than a year. Among other things encompassed by the study was the Executive Order governing the security classification program. A new Executive Order has just been issued. We in the Executive Branch are convinced that the changes in the security classification program embodied in the new Executive Order will result in substantial improvement in the program, although only experience will demonstrate the full range of their impact.

As I also pointed out earlier in my statement, the new Executive Order established an Interagency Classification Review Committee which has the responsibility to continuously review implementation of the program and suggestions and complaints in connection with the program,

from whatever source they arise. This insures that the review of the security classification system conducted over the last 14 months will not be a one-time effort, but rather a continuing process.

These are by no means, of course, the only reviews of the security classification program which are being conducted. Within the Department of Defense, a number of actions have been taken directly relating to the classification and protection of information. On July 1, 1970, the Defense Science Board submitted a report prepared by its Task Force on Secrecy to the Secretary of Defense. Among the questions addressed in that report were the classification of information in all stages of research, development, test and evaluation, as well as in procurement and deployment. Additionally, the Department of Defense Classification Review and Advisory Board was reactivated in December 1971 for the purpose of developing action programs covering declassification of specific bodies of material, establishment of basic guidelines for downgrading and declassification of hardware items, general policies covering classification of other than scientific and technical information, simplifying marking procedures for downgrading and declassification, and procedures for a prompt declassification of information released in Congressional testimony by Government officials.

In light of these reviews, both on a Government-wide and on a Departmental basis, and in light of the very substantial changes in the

security classification program initiated by the new Executive Order and actions of the Department, the Department of Defense does not believe that the creation of a further study commission relating to the national security and public information as proposed by H. R. 9853 is either necessary or desirable.

Mr. Chairman, this concludes my statement.

ILLEGIB