



**INFORMATION SECURITY
OVERSIGHT OFFICE**

**ANNUAL REPORT
TO THE PRESIDENT**

FISCAL YEAR 1979



12 1 APR 1980

President Jimmy Carter
The White House
Washington, D.C. 20500

Dear Mr. President:

The enclosed report represents the results of the first year of operation under your Executive Order on National Security Information.

As perceived by the Director of the Information Security Oversight Office, Michael T. Blouin, 1979 was to be a year of transition. This report, which covers the period under which Mr. Blouin served as Director, reflects that perception and attempts to point to the areas in which progress has been made, as well as where improvements are needed. It is not intended to be an exhaustive recitation of Executive Branch activity but rather a summation of the progress toward achievement of your stated goals.

I believe it is fair to say that much progress has been made. The past year has been a good beginning. Although many of your goals have not been fully accomplished, we are well on our way.

- An attitude of openness and cooperation is developing.
- It is too early to tell if fewer facts are being classified than prior to E.O. 12065, but it appears that information is being classified for a shorter period of time and that the great majority is being classified at the lowest level.

There is a substantial decrease in the number of people authorized to classify in the first instance and the use of guides is beginning to expand beyond previous Orders.

Agency actions to accelerate declassification have begun with a goal of meeting the 10-year target date.

However, this report speaks not just of progress but of problems as well some that may require your direct involvement in the future.

We have attempted to be objective and balanced in our assessment with one goal in mind -- to give you the state of the art of information security. I trust we have approached success in this regard.

Sincerely,

ROBERT W. WELLS
Acting Director

CONTENTS

SUMMARY	1
RECOMMENDATIONS	53
BACKGROUND	11
A. Need for the Order	11
1. Why Executive Order 12065?	11
2. Lessons Learned from Executive Order 11652	12
B. Development of Executive Order 12065	14
C. Transition Activities	15
II. INFORMATION SECURITY OVERSIGHT OFFICE	17
A. Establishment	17
B. ISOO's Perception of Oversight	18
III. FINDINGS	22
A. General	22
B. Program Implementation	23
1. Management	23
2. Classification	27
3. Declassification	43
C. Mandatory Review Requests and Appeals	47
D. Safeguards	48
E. Education and Training	50

LIST OF EXHIBITS

EXHIBIT 1 -- Agencies Monitored by ISOO	9
EXHIBIT 2 -- Number of Original Classification Authorities	29
EXHIBIT 3 -- Original Classification Authority	30
EXHIBIT 4 -- Estimated Number of Personnel Authorized to Apply Derivative Markings	32
EXHIBIT 5 -- Document Classification Decisions (Number)	36
EXHIBIT 6 -- Document Classification Decisions (Percentage)	37
EXHIBIT 7 -- Classification - Document Classification Decisions	40

SUMMARY

This constitutes the first report to be submitted by the Information Security Oversight Office (ISOO) to the President under E.O. 12065. The report covers the period December 1, 1978, through November 30, 1979, although the statistical data upon which much of the report is based was gathered during the period May - September, 1979. The use of the mid-year reporting period was based on the fact that the early months of 1979 saw a period of transition take place whereby agencies were adjusting to the new Order. In addition, the reporting procedure by which the statistics were gathered was not developed for use until late spring.

ISOO transition activities consisted of providing early training on the provisions of the Order and assisting agencies in complying with its administrative requirements. The time required of ISOO staff in assisting agencies in meeting the provisions of the new Order was made quite lengthy by virtue of the fact that under E.O. 12065, ISOO is required to actively oversee the information security program of 56 agencies and their components as compared with 37 under E.O. 11652.

In addition to assisting agencies in complying with the administrative requirements of the Order, the ISOO staff also conducted 123 inspections for which a formal report was written. These covered 52 agencies plus 25 major components and 25 staff offices of those agencies. There were also three inspections of field activities outside the Washington metropolitan area in Florida, California and Europe. These inspections provided the ISOO insight into the status of agency implementation, significant achievements, and problem areas.

This report attempts to measure the status of the executive branch information security program based on ISOO's perception of agency progress. Agency progress was measured through analysis of agency compliance with the administrative requirements of the Order, the findings of ISOO analysts during on-site inspections and statistics submitted to the ISOO by executive branch agencies. Listed below is a summary of those findings:

1. Significant changes were brought about in the information security program by the language of E.O. 12065. These were occasioned by experience with E.O. 11652 and lessons learned in administering the program under that Executive Order.

2. The development of the Order was done in the spirit of what it was to achieve -- openness in government. In an unprecedented step, the Order was made available to the public and the Congress for comment. The final product reflects many of the over-500 comments received.

3. The myriad of administrative requirements contained in the Order and the development of oversight responsibilities and procedures had an impact on prompt implementation.

4. The Order made changes to require that all executive branch agencies which handle national security information be monitored by the Information Security Oversight Office. This resulted in a significant increase in the number of agencies and major subordinate elements monitored by the ISOO and served as a basis for expansion of the ISOO staff from 8 to its proposed staffing of 20 personnel.

5. While most agencies required to develop implementing regulations did so, a number of the major agencies had not published their regulations in the Federal Register as required by the end of the reporting period. However, discrepancies between these regulations and the Order or ISOO Directive were resolved by close coordination between the agencies and the ISOO. It is anticipated that these regulations will appear in the Federal Register before the end of the second quarter of fiscal year 1980.

6. With the exception of two agencies, all monitored activities required to develop systematic review guidelines for 20-year-old information have had these guidelines approved by the Archivist of the United States and the ISOO. National Archives and Records Service is working closely with the two agencies to expedite development. Use of these guidelines should result in bulk declassification during the systematic review process.

7. Through coordination with executive branch agencies and the Archivist of the United States, the ISOO has developed proposed guidelines for the systematic review of foreign government information as it reaches 30 years of age. It is the intent of the ISOO to issue a single guideline for use throughout the executive branch rather than have each agency issue its own version. The use of a single version will promote the uniform declassification and control of foreign government information. The proposed guideline has been placed in the Federal Register for public comment with a goal of issuing the guidelines prior to April 1980.

8. During FY '79 the ISOO concentrated on conducting in-depth inspections of agency programs to determine the status of agency implementation and to assist agencies to the maximum extent in meeting the administrative requirements of the Order and the Directive. A total of 123 inspections were conducted for which formal reports were written. Within the time available to the analysts, national security information created by the agencies was randomly sampled to determine compliance with the Order. In addition, inspections were conducted in DOD facilities and DOD contractor facilities in Florida, California and Europe. Inspections in Europe also included U.S. Embassies in London and Bonn.

9. The ISOO has, in limited instances, been denied random access to information under the "third agency rule." Under this rule, ISOO analysts were denied access to information provided to the inspected agency by another agency. Such denial in these instances precludes the ISOO from giving total assurance that national security classification is used for its intended purpose. The ISOO is working with affected agencies to resolve this problem area.

10. A first analysis of the results of statistical reporting under the new Order indicates that the oversight body is obtaining data which more accurately reflects the classification activities of agencies than did the reporting requirements of E.O. 11652. Notwithstanding, in some instances the ISOO experienced difficulty in obtaining uniform compliance by agencies in providing requested data. Because of this, data could not always be compiled into meaningful statistics and was omitted from this Report.

11. In most agencies, responsible officials appear to be taking reasonable steps for managing their programs. However, in some instances increased emphasis is needed on developing viable self-inspection programs, centralizing control, and providing sufficient personnel and resources to effectively implement the program.

12. Agencies have taken progressive action to meet the President's direction that the number of original classification authorities be held to the absolute minimum. Since the last report prepared by the ICRC covering the year 1977, original classification authorities have been reduced from 13,302 to 6,927 -- a 48 percent decrease.

13. For the first time, the ISOO has gathered data to estimate the number of individuals in the executive branch that have the authority to apply derivative classification markings to national security information. Reported estimates indicate that nearly 241,000 persons have this authority.

14. Agencies have just begun to meet the mandate of the Order that classification guides be prepared to facilitate the identification and uniform classification of national security information. Successful implementation of this mandate will require close scrutiny by both the ISOO and agency security staffs. Moreover, a concerted effort in education and training will be required of those charged with the responsibility for preparing guides as well as those who must use them.

15. During a five-month test period during May - September, 1979, agencies were required to gather data regarding the number of original and derivative classification decisions made. An original classification decision is the initial determination that the information requires classification protection. A derivative classification decision on the other hand, is the application of markings from an original decision to a newly-generated document. Agencies reported this information by actual count except for DOD, CIA, and Justice, who were permitted to gather and report the data in accordance with approved ISOO sampling techniques. Reported results indicate that agencies originally classified in over 396,000 instances during the five-month period. The ISOO is encouraged that nearly three-fourths of these decisions placed the classification of the information in the lowest classification designation. As requested by the ISOO, agencies submitted an estimate of their derivative classification decisions for the same five-month period. They estimated that derivative classification occurred in over five and three-quarter million instances. This confirms the original estimate of the ISOO that derivative classification constitutes over 95 percent of all classification and points out the need for increased emphasis by the agencies and the ISOO on the derivative classification aspects of the Order.

16. Reported results of assigned durations of classification on original classification indicated that approximately 33 percent of the information was assigned a declassification or review date 6 years or less from the time of origination. Considering the newness of the program, this represents a step forward in meeting the President's goal of retaining classification for the

shortest time consistent with national security needs. It is impossible to compare the 33 percent figure with the statistics compiled under the old Order, because the duration of classification under the old system was determined by the level of classification; Top Secret - 10 years; Secret - 8 years; and, Confidential - 6 years. Therefore, statistics obtained for this report will establish a new data base for future reports.

Notwithstanding, the ISOO's analysis of this aspect of the program indicates that, in some instances, classifiers are assigning an automatic 6-year declassification date to some information that will not lose its sensitivity in that time frame. In addition, the practice of assigning a 6-year date for review may well bring about a review burden that agencies cannot meet with allocated resources.

17. As expected during this early phase of implementation, the ISOO identified many marking errors in randomly reviewing agency records. These primarily involved failure to indicate the classification of portions of a document, including the subject; instances of classification without authority; improper identification of the authority for classification; improper marking of working papers; continued use of markings prescribed by E.O. 11652; failure to record the authority and reason on documents extended beyond 6 years; and, the use of unauthorized terms in conjunction with one of the three authorized classification designations. It is anticipated that improved security education programs with emphasis on marking will substantially reduce the frequency of marking errors.

18. Agency actions to accelerate declassification of national security information were begun in 1979. Several major agencies such as CIA and State took progressive steps to establish new organizations to implement their declassification responsibilities under the Order. Both of these organizations involved the hiring of personnel familiar with the subject matter to be declassified and the establishment of formal rules for the functioning of the organizations. While action has only begun, both achieved some progress in the declassification of information during the year. The DOD improved on its own organizational procedures for systematic review and made commendable achievement in meeting the goal of the Order to increase declassification. During the year, the DOD reviewed nearly four million pages of classified information and declassified 72 percent. The National Archives declassification efforts resulted in the declassification of approximately 1.6 million

pages of documents withdrawn between 1972 and 1979 in accordance with the provisions of E.O. 11652. Thirteen million pages of 20-year-old records were systematically reviewed for declassification under the provisions of E.O. 12065 and over 500,000 pages of records over 20 years old were reviewed on behalf of individual researchers.

19. Reported results show that the public made use of the provisions of the Order that provide for mandatory review of information for declassification upon request. During the 5-month reporting period (May - September), agencies received nearly 1,000 requests for such review. Of the requests acted upon by the agencies during the year, nearly 83 percent were declassified in whole or in part. Similarly, progressive action was taken by the agencies to declassify national security information upon appeal from a denial to declassify such information. Of the appeal cases acted upon by the agencies during the year, nearly 75 percent of the cases resulted in declassification in whole or in part. Notwithstanding, the ISOO is concerned that agencies are not acting as promptly as they should on these cases. The Order provides in certain cases for the balancing of the public's interest in knowing information against the need to provide it continued security protection. Reported results indicate that this provision was applied in some instances during the year. Moreover, no complaints were registered by the public with the ISOO concerning the application of this provision.

20. The Order provides that the Director may issue waivers to requirements of certain provisions of the Order and the Directive. Issuance of such waivers was limited during FY 79. In each instance, a thorough investigation of the matter was made by the Director and the Deputy Director personally before the waiver was granted.

21. ISOO inspections indicated that increased emphasis is required by some agencies on the physical security aspects of the information security program. This includes emphasis on accountability, access and inventory of Top Secret material; control over reproduction of classified information; changing and control over combinations to security containers; and, necessary action to insure that security containers meet prescribed standards.

Discrepancies such as these appeared more often in smaller agencies that were new to the information security program and which had no trained security personnel. This area requires additional coverage in agency and ISOO security education programs.

22. An analysis of problem areas discovered during ISOO oversight inspections, indicates that emphasis is required in agency programs during FY 80 in the following order of priority:

- A. Agency management and oversight.
- B. Satisfaction of program administrative requirements.
- C. Security education training.
- D. Marking of national security information.
- E. Safeguarding national security information.
- F. Reduction of excess classified holdings.
- G. Security clearances.
- H. Declassification.

These priority items will be closely observed during the on-site inspections by ISOO analysts during FY 80. A formal inspection plan has been developed which places maximum emphasis on the conduct of inspections in the high priority agencies.

23. Agency personnel are cleared in numbers and at a level which appear to exceed agency needs. The cause appears to be attributed to a widespread lack of understanding concerning the relationships among investigative requirements, position sensitivity, and the granting of a clearance. This is resulting in a waste of funds expended for investigative purposes and personnel may be exposed to national security information for which they have no need-to-know.

In conclusion, the year 1979 was one in which both the ISOO and the agencies laid the foundation for subsequent development and implementation of the government's information security program. It proved to be a valuable learning experience, particularly for those agencies that were new to the program. Both the ISOO inspections and agency self-inspections have identified areas of weakness in agency programs that require increased emphasis and attention by top management officials. The vast majority of the administrative requirements of the Order and Directive have been met and agencies and the ISOO can now begin to devote full-time efforts to the mechanics and the day-to-day operation of the program. There were both problems and accomplishments

in 1979 but progress was made toward the achievement of the President's goal of instilling credibility in the system. Moreover, the in-depth review and inspection of agency programs by the ISOO has provided the oversight body with a viable base upon which to gauge agency progress in the future. The ISOO looks forward to 1980 and is confident that agencies will make continued progress during that year toward achieving the goals of Executive Order 12065.

EXHIBIT 1

AGENCIES MONITORED BY ISOO
(Alphabetical by Agency-Plus Abbreviation/Acronym Assigned)

<u>AGENCY</u>	<u>ABBREVIATION ACRONYM</u>
1 Action	ACTION
2 AGENCY FOR INTERNATIONAL DEVELOPMENT (S)	AID
3 Agriculture, United States Department of	USDA
4 Board for International Broadcasting	BIB
5 CENTRAL INTELLIGENCE AGENCY (TS)	CIA
6 Civil Aeronautics Board	CAB
7 COMMERCE, UNITED STATES DEPARTMENT OF (S)	COMMERCE
8 Commodity Futures Trading Commission	CFTC
9 DEFENSE, DEPARTMENT OF (TS)	DOD
10 ENERGY, DEPARTMENT OF (1) (TS)	DOE
11 Environmental Protection Agency, United States Executive Office of the President	-EPA
12 COUNCIL OF ECONOMIC ADVISORS (S)	CEA
13 INTELLIGENCE OVERSIGHT BOARD (TS)	IOB
14 NATIONAL SECURITY COUNCIL (TS)	NSC
15 OFFICE FOR MICRONESIAN STATUS NEGOTIATIONS (S)	OMSN
16 Office of Administration (2)	OA
17 OFFICE OF MANAGEMENT AND BUDGET (TS)	OMB
18 OFFICE OF SCIENCE AND TECHNOLOGY POLICY (TS)	OSTP
19 OFFICE OF THE SPECIAL REPRESENTATIVE FOR TRADE NEGOTIATIONS (TS)	OSRTN
20 OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES (TS)	OVP
21 EXPORT-IMPORT BANK OF THE UNITED STATES (C)	EXIMBANK
22 Farm Credit Administration	FCA
23 Federal Communications Commission	FCC
24 FEDERAL EMERGENCY MANAGEMENT AGENCY (3) (TS)	FEMA
25 Federal Energy Regulatory Commission (4)	FERC
26 Federal Home Loan Bank Board	FHLBB
27 Federal Maritime Commission	FMC
28 Federal Reserve System	FRS
29 Foreign Claims Settlement Commission of the United States	FCSC
30 GENERAL SERVICES ADMINISTRATION (TS)	GSA
31 Health, Education and Welfare, Department of	HEW
32 Housing and Urban Development, Department of	HUD
33 Interior, United States Department of the	INTERIOR
34 INTERNATIONAL COMMUNICATION AGENCY, UNITED STATES (5) (S)	USICA
35 Interstate Commerce Commission	ICC
36 JUSTICE, DEPARTMENT OF (TS)	JUSTICE
37 Labor, United States Department of	LABOR
38 Marine Mammal Commission	MMC
39 NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (TS)	NASA
40 National Credit Union Administration	NCUA

EXHIBIT 1
(Continued)

<u>AGENCY</u>	<u>ABBREVIATION ACRONYM</u>
41 National Science Foundation	NSF
42 National Transportation Safety Board	NTSB
43 NUCLEAR REGULATORY COMMISSION, UNITED STATES(6)(TS)	NRC
44 Office of Personnel Management (7)	OPM
45 OVERSEAS PRIVATE INVESTMENT CORPORATION (C)	OPIC
46 Securities and Exchange Commission	SEC
47 Selective Service System	SSS
48 Small Business Administration	SBA
49 STATE, DEPARTMENT OF (TS)	STATE
50 Tennessee Valley Authority	TVA
51 TRANSPORTATION, DEPARTMENT OF (S)	DOT
52 TREASURY, DEPARTMENT OF THE (TS)	TREASURY
53 UNITED STATES ARMS CONTROL AND DISARMAMENT ADMINISTRATION (TS)	ACDA
54 United States International Trade Commission	USITC
55 United States Postal Service	USPS
56 Veterans Administration	VA

NOTE: Agencies printed with capital letters have been granted original classification authority.

I FINDINGS.

This is the first report submitted by the Information Security Oversight Office (ISOO) to the President describing the status of the executive branch's information security program. The report covers the period December 1, 1978, through November 30, 1979. For reasons explained in this report, the statistical data cited on the program was gathered during the period May - September, 1979.

The purpose of this report is to inform the President of the state of the information security program in the executive branch including the status of agencies' implementation, the effectiveness of implementation, problem areas that exist within the program, and ISOO's perception of how these problems should be addressed.

A Need for the Order

1. Why Executive Order 12065?

Executive Order 12065 was not a new concept. It was preceded by four different Executive Orders relating to information security and security protection. These orders included Executive Order 9835 issued in 1947, Executive Order 10290 in 1951, Executive Order 10501 in 1953 (amended several times), and Executive Order 11652 in 1972. Each Order attempted to improve upon the others, including efforts to improve protection for national security information as well as developing improved and more efficient methods and procedures for program management. Each made important contributions toward achieving these goals. One problem with previous Orders has been that a philosophical commitment was made to build a system for protecting national security information without incorporating a viable mechanism or procedure to ensure that executive branch agencies were effectively implementing the system.

A more serious deficiency was that previous Executive Orders did little to promote public accessibility through declassification once national security information had lost its sensitivity. Moreover, there was no assurance that information classified and protected by agencies as vital to the national security was in fact deserving of such protection. Also lacking

were detailed criteria for determining what should be protected as national security information. These shortcomings were of prime importance to President Carter and are reflected in his guidance for developing an information security program that not only protected national security information but also protected the right of public access to information concerning the affairs of government.

2. Lessons Learned from Executive Order 11652

Although Executive Order 11652 did attempt to bring enforcement to the information security program by establishing the Interagency Classification Review Committee (ICRC) as the oversight body, implementation of the Order did not achieve the results intended. Overclassification, unnecessary classification and classification for periods longer than required continued. Simply put, public credibility and that of our foreign allies in the government's information security program was lacking. The fact that every item of business relating to the administration of the Order, including suggestions and complaints from agencies or the public, had to be considered by the full oversight committee often resulted in a slow and cumbersome process.

The ICRC consisted of a Chairman and seven members representing the Departments of Defense, Energy, Justice and State, the National Archives and Records Service, the Central Intelligence Agency, and the National Security Council staff. Thus, the Committee was comprised of representatives of the agencies that classify the vast majority of the nation's security information, thereby limiting their apparent authority to objectively oversee and enforce the program. This greatly compounded the problems faced by the staff of the ICRC in monitoring the very agencies that assisted the National Security Council in providing policy direction to the program. This problem was addressed by the General Accounting Office in a report issued March 9, 1979: "Improved Executive Branch Oversight Needed for the Government's National Security Information Classification Program."

The ineffectiveness of the ICRC can also be attributed in part to its lack of status in any organizational structure, a fact that caused some departments to treat lightly the Committee's authority.

While the ICRC did an effective job in assisting agencies' implementation of the Order and brought some semblance of structure to the information security program, the lack of any real authority to enforce compliance precluded the ICRC from effectively carrying out its oversight role.

In addition to the obvious need for improved oversight, analysis of the program under Executive Order 11652 showed some weaknesses. In many sections of the Order the language was vague and permissive, or failed to address specific areas. Many agency programs lacked sufficient personnel and resources to effectively carry out the mandates of the Order, despite the requirements of the National Security Council directive that adequate personnel and funding be made available. The lack of a firm requirement in the Order for issuance of written classification guidance impeded consistency in classification and contributed to abuse of the system. The marking requirements of the Order were complex which made it difficult to mark information and to train personnel in the system. The Order failed to address or prohibit the use of markings such as "agency" or "conference" in conjunction with the three markings approved for identifying national security information. The use of these additional markings confused recipients of the information as to the protection the originator intended to be given to such information and, through subsequent derivative classification based on such documents, resulted in the proliferation of unnecessarily classified information.

A major shortcoming in Executive Order 11652 was its failure to mandate that portions of classified documents be marked to indicate the level of classification of those portions. Consequently, most Departments indicated only the overall classification of the document. Since the vast majority of information is classified on a derivative basis, this practice resulted in unnecessary classification and overclassification of information. While the information extracted from such documents and used in new documents may have been unclassified and therefore possibly subject to public accessibility, the generator of the derivative document had no way of determining this and was compelled to apply the overall classification level of the source document to the derivative product.

A serious problem in the effective monitorship of E.O. 11652 was the inability of the ICRC to obtain reliable statistical data regarding the program. Some major agencies contended that they could not economically provide data that the Committee requested. Some adopted sampling systems that provided only a partial reporting of the total classified volume; others failed to report the distribution of documents placed into the various declassification schedules that existed under E.O. 11652. Since these sampling systems were approved by the Committee, the ICRC staff was unable to develop a reliable base upon which to measure program progress. Experience with this system showed that future statistical gathering approaches would have to be less cumbersome than that required by the six-page report form under E.O. 11652 and capable of providing a reliable reflection of agency classification and declassification actions. Without reliable statistical data, neither the President, the Congress, the public, nor the agencies themselves can be cognizant of the state of the program.

Experience also showed that agencies overused those provisions of E.O. 11652 that permitted them to exempt information from the automatic declassification provisions of the Order. Moreover, the permissive language of that Order resulted in a great majority of the information being marked with no definitive declassification or review date. Thus, while the intent of the Order was for most information to be declassified in ten years or less, the majority was marked for retention of classification for 30 years or longer.

B. Development of Executive Order 12065

Upon taking office, President Carter initiated action to review the Government's information security program. On June 1, 1977, the President issued Presidential Review Memorandum 29 (PRM-29) which established a government task force to conduct a comprehensive review of the program throughout the executive branch. PRM-29 directed that a new Executive Order be developed which would simplify the system, result in public and foreign government credibility, and provide improved security protection for essential national security information.

The first draft of the proposed Executive Order was forwarded to executive branch agencies on September 13, 1977. In an unprecedented step, the proposed Executive Order was also made available to organizations and individuals outside the executive branch, including Committees of the Congress, for review and comment. Over 500 comments were received and after review many were incorporated into the second draft of the Order. Final differences were resolved during a meeting of the Special Coordinating Committee in April 1978.

Executive Order 12065 was issued on June 28, 1978, with an effective date of December 1, 1978. This Order went through a process subjecting it to more scrutiny, both from within and outside government, than any previous Order. The Executive Order was conceived with the same theme it was meant to achieve -- openness. Specific goals of the Order reflect that theme:

- Emphasis should be to limit classification and to accelerate declassification.
- All documents should be declassified as early as national security permits. A justification for the extension of classification beyond six years is required.
- Information may be classified only if its release can reasonably be expected to cause identifiable damage to the national security.
- Declassification should be given emphasis equal to that afforded to classification.
- Classification authority should be held to a minimum.
- Training on the Order should be emphasized within each agency.

C Transition Activities

During the period between the issuance of the Order on July 3, 1978, and the effective date of December 1, 1978, the ICRC staff began preparing the way for the implementation of E.O. 12065. Their primary objective was to provide an orderly transition to the new Order and to have the new Information Security Oversight Office operational on December 1, 1978.

A most important aspect of transition was the development and issuance of the ISOO directive implementing the Order. Since early implementation by agencies depended upon their prompt receipt of the directive, the ICRC and its staff gave high priority to its development and promulgation. This process followed closely the procedures and task force organization used to develop E.O. 12065. The directive was closely coordinated with interested Congressional Committees and contains substantive provisions recommended by those Committees and Subcommittees.

The Information Security Oversight Office Directive No. 1 was finalized and published in the Federal Register on October 5, 1978. The finished product seeks to expand and clarify those sections of the Order where needed and to provide additional administrative procedures relating to classification, declassification and safeguarding of national security information.

Following promulgation of the Directive, the ICRC staff turned its attention to the myriad of other duties that were required to be accomplished before the December 1, 1978, effective date. For example, under the provisions of E.O. 12065, the ISOO would be required to monitor the program of any executive branch agency that handles classified national security information; this is contrast to the ICRC's monitoring of only those agencies with original classification authority. The ICRC staff conducted a survey of all agencies, offices, committees, etc. listed in the Government Organizational Manual. Based on the results of the survey, staff visits were made to all organizations that appeared to have classified material. Upon completion of necessary coordination, it was determined that the ISOO would be required to actively oversee the information security programs of 56 agencies and their major components as compared with 37 under E.O. 11652.

Other transitional activities undertaken by the staff included development of policies and procedures for ISOO inspections, scheduling of inspections, establishing requirements for agency reporting to the ISOO, initial coordination for the developing of reporting forms, making the necessary administrative arrangements for transfer of the ICRC staff to the ISOO and for expanding the staff. Additional activities included revising office instructions and procedures to incorporate new responsibilities under the Order, disposition of ICRC records and establishing ISOO records in accordance with appropriate

records management procedures, and physical relocation of the office from the National Archives and Records Service to the General Services Administration Building.

II. INFORMATION SECURITY OVERSIGHT OFFICE

A. Establishment

In issuing the new Order, the President made it quite clear that compliance with the provisions of his new Order was essential: "..., I have created an Information Security Oversight Office to provide overall supervision . . . The Office will report regularly to the National Security Council and to me on compliance with the Order. The Office is a key element to the new classification system, and it will have my strong support."

As pointed out earlier, the placement and lack of independent stature of the ICRC contributed materially to its inability to provide effective oversight. Consequently, placement and the overall structure of the ISOO within the executive branch was considered to be of great importance. The final arrangement placed the Office within the General Services Administration for administration with policy direction coming from the National Security Council.

The Director of the ISOO is granted independent authority in implementing the Order, with the exception that some decisions made by the Director are subject to appeal by the agencies to the National Security Council. All directives prepared by the ISOO mandating compliance by agencies must be approved by the National Security Council.

The Order also establishes an Interagency Information Security Committee (IISC), chaired by the ISOO Director. The IISC is comprised of representatives of the major agencies involved with national security information and serves as an advisory body to the Director on implementation of the Order.

The day-to-day oversight of implementation of the Order is carried out by the ISOO through its Director and staff. Although the effective date of the Order was December 1, 1978, the Director of the ISOO was selected in January and appointed in March 1979. During the interim, the former Executive Director of the ICRC served in the capacity of Acting Director and its staff of 8 transferred to form the nucleus of the new ISOO staff. This utilization

of the ICRC staff proved to be a valuable asset in assuring a smooth transition to the new system. Not only did they have a good working knowledge of the Order and the necessary know-how to assure its effective implementation, but the rapport and mutual sense of cooperation they had developed with agency security staffs was invaluable in making the changes introduced by the new Order less disruptive. By August 1979, ISOO staff strength reached 11. Four additional program analysts joined the staff in January 1980 and three more professionals are expected to join the staff before the third quarter of FY 1980 ends. This increase in personnel staffing represents strong Administration support for increasing the effectiveness of the Office.

B. ISOO's Perception of Oversight

In developing its approach for meeting its assigned oversight role, the ISOO first attempted to view the realities of the Order in terms of what had to be achieved in the short run; and then to institute an approach which would make it clear that the President's goals, as he had envisioned them, were to be attained.

By implication, the Order itself had set up a priority list of actions to be taken. Agencies were required to develop regulations and systematic review guidelines, the latter for both United States information and foreign government information. The Order also required that agencies with special access programs review those programs and to continue them only in accordance with the provisions of the Order. By July 1, 1979, agencies were required to establish a system of accounting for these programs.

A first priority of the ISOO was to assist in complying with the administrative requirements of the Order described above. Although no specific date for promulgation of agency regulations was established in the Order, the Director of the ISOO informed all agencies that their regulations should be approved by the ISOO and in the hands of the Federal Register by September 2, 1979. Throughout 1979 the ISOO staff spent considerable time and effort reviewing and commenting on agency regulations. In most cases, this required at least four exchanges of correspondence before the ISOO was satisfied that all portions of the regulations were in agreement with the Order and the ISOO Directive. (The status of agency regulations can be found in Section III of this report).

The ISOO staff, in coordination with the National Archives, also spent considerable time reviewing and commenting on systematic review guidelines prepared by the agencies. Most agencies were able to meet the mandate that such guidelines be developed within 180 days after the effective date of the Order. (See Section III of the Report for a more detailed summary).

Section 3-404 of the Order requires that agencies develop, in consultation with the Archivist of the United States, guidelines for the systematic review of foreign government information. ISOO Directive No. 1 requires that these guidelines be developed within one year of the effective date of the Order. In working with the agencies and the Archivist, the Director of the ISOO took the position that the interests of uniformity and control over foreign government information would best be served by the development and issuance of a single, uniform guideline applicable to all agencies. After a series of meetings with the major agencies affected, a final draft was developed before the one-year deadline. The draft was forwarded to heads of agencies for their official concurrence and was also placed in the Federal Register for agency and public comment.

By far, planning for ISOO oversight centered around the conduct of detailed on-site inspections of agency information/security programs. The intent was to determine at an early stage the status of implementation within the agencies and, in some instances, to assist agencies in the development of their regulations and programs.

The ISOO inspection program was designed to have the ISOO analysts randomly review an agency's classified holdings (those created after December 1, 1978) to determine agency compliance. The first round of inspections was not as comprehensive as the Office would have liked because of the time spent by the ISOO staff on activities associated with administrative compliance by the agencies.

By and large, ISOO analysts were afforded unrestricted access to agency classified holdings. In a limited number of cases, agencies invoked the "third agency rule" thus precluding ISOO analysts access to classified information provided to the inspected agency by another agency. Current negotiations are being conducted with affected agencies to resolve this access problem. While the "third agency rule" has made oversight more

complex and time demanding in the few instances it has been invoked, it has not substantially detracted from the ability of the Office to perform its oversight role.

Drawing on the experiences of the former ICRC, ISOO planners developed an approach to collection of agency statistics designed to ensure that more reliable data would be obtained from agencies. As a first step, an experimental reporting form was developed for use during the period May - September 1979. The form was a single page rather than six separate reports as used under E.O. 11652 and was limited in its requirements to that information that the ISOO determined to be essential in order to develop a reliable base upon which to measure future program progress. Moreover, the statistics reported by the agencies will provide an indication of areas that should be given increased attention in future ISOO inspections. (An analysis of statistics gathered can be found in Section III of this report).

Agencies obtained the data by actual count with the exception that the data concerning document classification decisions from DOD, Justice (FBI), and CIA are projections based on sampling methods approved by ISOO. After review and recommendations by statistical analysts in both GSA and Commerce, ISOO approved for DOD a general sampling design which would utilize 1000 randomly-selected activities. DOD actually utilized 1005 randomly-selected activities that made a count for 21 consecutive days during September 1979. ISOO also approved a sampling design for FBI in which all original classification authorities (185 total) counted all classified documents they generated (both original and derivative) for 8 specified days during August and September 1979. In the case of CIA, ISOO approved use of an actual count of all classified documents generated within the agency for a 7-day period in September 1979. Through the use of the statistical sampling, the agencies used the data gathered to project the total classified activity within the agency for the 5-month period.

In developing an oversight approach for the year, ISOO was cognizant of the fact that staff and budget limitations under previous Orders had precluded the conduct of oversight inspections outside the Washington metropolitan area. Thus, in formulating the approach to inspection for 1979, ISOO developed its budget needs to take into account the need for in-field inspections.

During 1979, in addition to reviews in major agency headquarters, inspections were also conducted in DOD contractor facilities in Florida and California. In the fall of 1979 a detailed inspection was conducted at major military commands and Department of State activities in Europe. These inspections included a review of over 15,000 documents and in-depth discussions with classifiers.

ISOO envisions the 1979 inspection activities as only the beginning and has already scheduled inspections for 1980 for government and contractor activities in Atlanta, St. Louis, Philadelphia, Norfolk, and the Providence/New Haven areas. Additional field inspections will be scheduled as the ISOO staff expands.

Visits were also made to major Congressional Committees which handle classified information. These visits showed that, while physical security procedures and facilities varied from Committee to Committee, physical security protection for the material appeared adequate. Access to classified holdings was limited and strict controls were employed for document dissemination. The Committees acknowledged however that they had little control over the knowledge that a Member or staff person attains from working with classified information.

Certain foreign governments also expressed concern over the Order during 1979. ISOO arranged for a British team to visit with executive branch agencies and Congressional Committee personnel to discuss the impact of both the Order and the Freedom of Information Act on protection of British information provided to the United States in confidence. The visit proved reassuring to the British team that the Order did not weaken the ability of the United States to protect United Kingdom information.

All in all, the approach to oversight developed by the ISOO for 1979 was one of getting the program started. It was realized at the very beginning that the year could prove frustrating in terms of establishing an overall, effective oversight program. Agencies needed time to start their own programs. Personnel had to be educated and trained in the new specifics of the Order; regulations and other administrative requirements also had to be met. Nevertheless, the approach for oversight developed for 1979 did provide creditable oversight and laid the basis for a much more ambitious program in 1980.

III. FINDINGS.

A. General

As the previous sections of the Report have indicated, 1979 was a year of transition. As in all new organizations, the necessary planning, coordination, development of rules and procedures, and actual establishment of organizational structure and lines of supervision had a significant impact on the prompt implementation of the Order.

While agencies could begin the basics of developing their implementing regulations after issuance of the Order, they could not finalize those regulations until issuance of the ISOO Directive in October 1978. Other delays were caused by the fact that the January appointment of the Director of the ISOO was not approved until March 1979. Many of the decisions regarding the operations and requirements of the Office were thus held in abeyance pending approval of his appointment. For example, administrative requirements for the development, coordination and issuance of the first test form for reporting statistical data took until mid-April 1979.

Those agencies that had been subject to ICRC oversight under E.O. 11652 had a distinct advantage in the development of regulations and the fulfillment of other administrative requirements of the Order. They had trained information security professionals who could begin working on implementation. The new agencies that became subject to oversight under E.O. 12065 not only lacked trained personnel, but had virtually no background on which to base the development of regulations for their program. Both old and new agencies were required to initiate extensive training programs to familiarize their personnel with the provisions of the Order and the ISOO Directive.

The ISOO staff attempted to provide maximum assistance to these training efforts. In early January 1979, the staff conducted a one-day information security training session for security managers of all executive branch agencies. The staff also made individual orientation visits to many agencies to review training programs and to assist agencies in the development of such programs. Recommendations were made to change or improve the programs where needed.

During 1979, the ISOO staff conducted 123 inspections for which a formal report was written. These covered 52 agencies plus 25 major components and 25 staff offices of these agencies. In addition, there were three inspections of field activities outside the Washington Metropolitan area -- in Florida, California, and Europe. The ISOO staff also conducted 18 follow-up inspections. Formal reports covering the inspections were forwarded to agency senior officials by the Director, ISOO. These reports provided the basis for the ISOO's analysis of the status of agencies' implementation, significant achievements, problem areas and recommendations for improvement of the program. Experience has shown that a number of agencies have not informed the ISOO of actions taken to place the ISOO recommendations into effect as requested. Nevertheless, verification of agency action taken, if any, has been a regular part of subsequent ISOO inspections of these agencies. These have disclosed that agencies have, in most instances, initiated responsive action to resolve the problem areas. In a limited number of cases, agencies have failed to initiate the necessary action to resolve cited problem areas. The ISOO was particularly concerned about the failure of the Department of Commerce to take responsive action to the recommendations cited in ISOO inspection reports covering the Department's information security program. It should be noted, however, that the ISOO is encouraged by action initiated by the Department's new Secretary, Philip Klutznick, and the personal interest he has taken to resolve the problem areas expeditiously.

B. Program Implementation

1. Management

The success or failure of any program depends upon the effectiveness of its administration and the support the program receives from top management. In carrying out its oversight role, the ISOO has stressed the need for agencies to develop and effectively operate their own oversight programs. Dedicated and effective agency self-inspection is the best means of assuring that the provisions of the Order are being carried out.

Experience has shown that the best arrangement for assuring an effective information security program is to coordinate staff supervision of all agency security functions in one unit wherever possible. However, ISOO inspections revealed that in some agencies, responsibility for various aspects of the

program were fragmented. In these instances ISOO recommendations were made for more centralized control. In a limited number of instances, lack of compliance with the requirements of the Order and the Directive clearly stemmed from the lack of interest and support at top management levels.

As required by the Order, all agencies have designated a Senior Official to monitor implementation. However, ISOO inspections disclosed that some agencies need improved oversight. For example, agency self-evaluation of staff and field activities did not always include coverage of the information security program. Further, in those instances where coverage was included, agencies did not always fully utilize evaluation findings to modify the program where necessary or to bring problems discovered to the attention of top management. Another agency oversight function that requires increased emphasis is the establishment of viable systems for reviewing classified information generated to verify the propriety of classification and the correctness of markings. During the year, the ISOO staff had considerable success in rectifying this problem in smaller agencies by encouraging those agencies to establish central points for control, review and application of classification markings.

In some cases, recommendations were made to senior officials that additional personnel or resources be made available for their information security programs. These deficiencies were compounded in some instances when personnel in charge of the program were given a myriad of additional duties. For example, in the Department of Commerce only a limited number of personnel were available during the report period to administer the program on a full-time basis for over 3,000 offices. Yet, these same personnel were actively involved in duties such as providing physical security to the Secretary or conducting investigations unrelated to the information security program. In these situations, these personnel were left little time to establish or monitor the information security program or to conduct security training within their organizations. As mentioned earlier, the new Secretary of Commerce appears to be taking responsive action to rectify this problem.

One indication of an agency's dedication to and support for the information security program can be found in an analysis of its compliance with the administrative requirements of the Order and the Directive. The implementing regulations of all agencies required to develop and publish such regulations have been approved by the ISOO except for the Department of Commerce, EPA, USDA, FEMA, and ACTION. Neither Commerce nor EPA have submitted drafts for approval. The regulations of EPA and FEMA are being delayed because of agency reorganization. In the case of USDA, FEMA, and ACTION, initial drafts have been reviewed and commented on by the ISOO but final approval has not been given.

The ISOO has approved the regulations of six other agencies subject to the incorporation of changes recommended by the Oversight body. These regulations include those of the Department of Defense, Justice, HEW, DOE, DOT and the CIA. It is anticipated that necessary revisions and publication in the Federal Register will occur for DOD and CIA prior to the start of the third quarter of FY 80. Publication of the other regulations is being delayed by coordination and approval within the cited agencies.

The Regulation that DOD will publish in the Federal Register will be the original version adopted by that Department -- the version upon which DOD elements developed and promulgated their supplemental regulations. ISOO has been informed that the DOD regulation will not contain recommended ISOO changes but that such changes will appear in a subsequent publication following their coordination within DOD. The delayed publication of the DOD regulation has resulted, according to some contractors interviewed by ISOO personnel and a security representative of a major DOD contractor, in significant implementation problems within Defense industry. The Department of Defense has, however, worked closely with the Council of Defense and Space Industries, National Classification Management Society and the American Society for Industrial Security to reduce or eliminate uncertainties and inconsistencies regarding the program in Defense industry.

The purpose of the systematic review guidelines required to be developed by agencies is to expedite the declassification process and to achieve consistency in the declassification of material. The guidelines prescribe specific categories of information that cannot be automatically declassified

as they become 20 years old. Information falling into these categories is reviewed item-by-item to determine if continued classification beyond 20 years is required. Only the head of an agency can continue the classification beyond 20 years. The guidelines may be applied to 20-year-old material by the Archivist of the United States, the originating agency and any other agency authorized to do so by the originating agency. The application of these guidelines should result in automatic declassification of information that does not meet the parameters of the guidelines.

The ISOO and the National Archives and Records Service (NARS) took steps early in the program to remind agencies of their responsibilities to develop the systematic review guidelines within 180 days after the effective date of the Order. In-depth meetings were conducted between NARS and agency representatives to develop more uniform procedures and formats.

There are 37 agencies in the executive branch that have cognizance over information 20 or more years old. Of these, 35 have developed systematic review guidelines that have been approved by NARS and ISOO. Only the National Security Council and the Office of Science and Technology Policy have not had their guidelines approved. In both cases, the agencies have developed guidelines but certain aspects of those guidelines require additional change to meet the requirements of the Archivist of the United States and the ISOO. It should be also noted, however, that NARS is working closely with the two agencies to expedite development. On October 25, 1979, 17 of the 37 agencies published their systematic review guidelines in the Federal Register as required by Section 5-402 of Executive Order 12065. The remaining 18 agencies have been directed to publish in the Federal Register as soon as possible.

Both NARS and the ISOO realize that this first attempt at writing systematic review guidelines has resulted in rather broad guidance in some instances. However, both feel that as additional experience is gained on a day-to-day basis working with systematic review, further refinement of the guidelines can be accomplished. Achievement of this goal will be made a part of the ISOO inspections and close scrutiny will be given to the guidelines during their review every two years.

The Order specifies that within 180 days of the effective date of the Order, all agencies with Top Secret originating authority review all existing Special Access Programs. Interim reports showed that of all the agencies with Top Secret originating authority, only the Department of Defense and the Central Intelligence Agency originate any Special Access Programs. The Central Intelligence Agency established a National Foreign Intelligence Board (NFIB) Working Group on Compartmentation to conduct a review of all intelligence community programs for controlling compartmented intelligence. To date, CIA proposals have been before the NFIB and are presently being revised in accordance with NFIB discussions. It is anticipated that proposed revisions will be completed in the near future and that such revisions will be forwarded to ISOO. The Department of Defense has their accounting program established. To date, they have reviewed and continued 43 existing Special Access Programs and have added only one additional program. Work is continuing to complete the detailed review and they will advise the ISOO upon its completion.

2. Classification

a. Original Classification Authority. Executive Order 12065 restricts the delegation of original classification authority to principal subordinate officials who have a frequent need to exercise such authority. An original classification authority is an authorized individual in the executive branch who initially determines that particular information requires a specific degree of protection against unauthorized disclosure in the interest of national security. The Order requires that the delegation of original classification authority be held to an absolute minimum and that periodic reviews be conducted to ensure that officials so designated have demonstrated a continuing need for such authority. The Order also prohibits the redelegation of delegated authority.

Agencies have made a concerted effort to reduce the number of officials with original classification authority. Since the last published ICRC Report covering 1977, the number of officials with original Top Secret authority (1492) has remained relatively constant but the number of original Secret classification authorities has been reduced from 8,247 to 3,883 -- a 53 percent decrease.

Similarly, original Confidential classification authorities have been reduced from 3,657 to 1,552 -- a 58 percent decrease. Overall, since 1977, original classification authorities have been reduced from 13,302 to 6,927 or nearly 48 percent. Examples of agency achievements in this area include: AID, 32 percent; DOD, 39 percent; DOE, 95 percent; and, USICA, 45 percent. These significant reductions are indicative of executive branch agencies' desires to meet the President's direction to keep the number of original classifiers at an absolute minimum. (See Exhibit 2 and 3).

Monitorship of agency actions in delegation and review of original classification authorities has been a regular part of ISOO inspections. Some instances have been identified where officials are not exercising their delegated original classification authority and ISOO analysts have made recommendations that such authority be withdrawn.

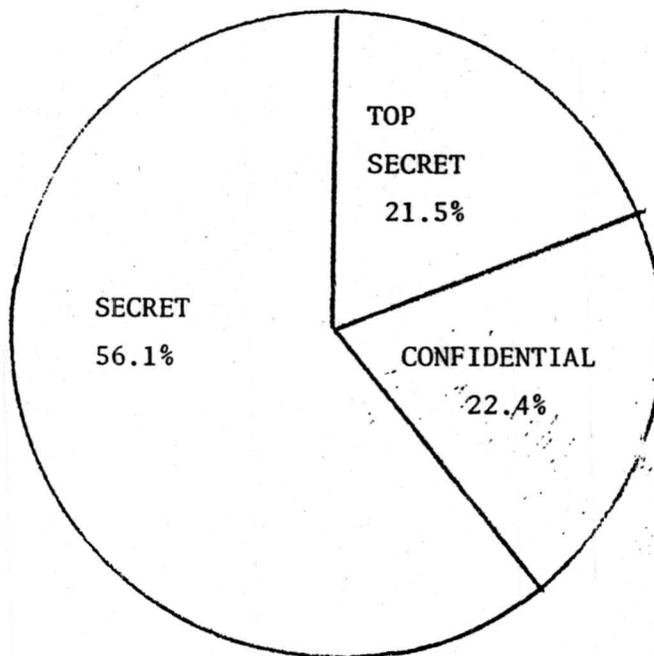
EXHIBIT NO. 2

NUMBER OF ORIGINAL CLASSIFICATION AUTHORITIES

AGENCY	TOP SECRET	SECRET	CONFIDENTIAL	TOTAL
1. ACDA	9		21	65
2. AID (1)				160
3. CIA	474		19	1664
4. COMMERCE			17	34
5. DOD	474		770	2323
6. DOE (2)	24			226
7. DOT				6
8. EXECUTIVE OFFICE OF THE PRESIDENT (3)	14		6	77
9. EX/IM BANK			6	6
10. FEMA (4)	1			
11. GSA	1	4		5
12. JUSTICE	235	173		408
13. NASA	4	29		33
14. NRC	6	31		37
15. OPIC (5)				
16. STATE	234	773	603	1610
17. TREASURY	16	6	90	112
18. USICA (6)		140	20	160
GRAND TOTALS -----	1492	3883	1552	6927
PER CENT -----	21.5	56.1	22.4	

- (1) Does not include IDCA personnel authorized October 1, 1979 (9 SECRET)
- (2) Established by the Department of Energy Organization Act, approved August 4, 1977, and effective October 1, 1977, pursuant to Executive Order 12009. Absorbed the energy research.
- (3) Includes eight offices: CEA, IOB, NSC, OMB, OMSN, OSTP, OSRTN, and the Office of the Vice President.
- (4) Established by Reorganization Plan No. 3, effective April 1, 1979, pursuant to Executive Order 12127, formerly the Federal Preparedness Agency (FPA).
- (5) No data submitted.
- (6) Established April 1, 1978, by Authority of Reorganization Plan No. 2 of 1977. Formerly the United States Information Agency (USIA).

EXHIBIT NO. 3
ORIGINAL CLASSIFICATION AUTHORITY



Top Secret Classification Authorities	-----	1492
Secret Classification Authorities	-----	3883
Confidential Classification Authorities	-----	1552

b. Derivative Classification Authority. Derivative classification is the determination that information is in substance the same as information currently classified, coupled with the designation of the level of classification. This subject was not included in previous Executive Orders or reporting requirements. The results reported by agencies reflect that there is wide variance among agencies with regard to the authority to apply derivative classification markings. Some agencies such as CIA and DOE limit derivative classification authority to designated officials. Other agencies reported that all personnel with appropriate security clearances may apply derivative markings. Still others, such as DOD, report that derivative authority is exercised only by individuals with appropriate clearances who also have the authority to approve documentation created within their organizations.

Agencies reported to the ISOO that an estimated total of 240,925 personnel have the authority to apply derivative classification markings. (See Exhibit 4). This figure compared with the 6,927 authorized original classifiers clearly indicates that both agency and ISOO oversight must concentrate on the derivative classification aspects of the program; ISOO analysts will continue to encourage agencies to limit derivative authority to designated individuals based on the belief that such designation will result in fewer derivative actions and improved uniformity in the program.

c. Classification Guides. The Order requires that each agency with original classification authority promulgate classification guides that will facilitate the identification and uniform classification of information requiring protection under the provisions of the Order. This mandate was not included in previous Orders governing the information security program.

Except for major agencies such as DOD and DOE, executive branch elements have not promulgated or used classification guides prior to the effective date of E.O. 12065. This subject presents a major education task to both the agencies and the ISOO. Consequently, the preparation and use of guides was made a major topic at the all-day training seminar conducted by the ISOO in November 1979.

EXHIBIT NO. 4

ESTIMATED NUMBER OF PERSONNEL AUTHORIZED TO APPLY DERIVATIVE MARKINGS

AGENCY	TOP SECRET	SECRET	CONFIDENTIAL	TOTAL
1. ACDA		98		98
2. ACTION				
3. AID (includes IDCA)	3671			
4. BIB				
5. CAB	6	19	8	33
6. CFTC				
7. CIA				
		ISOO WAIVER GRANTED		
8. COMMERCE	40	300+	400+	740+
9. DOD	55053	85016	29604	169673
10. DOE	8	3592	915	4515
11. DOT		368	-	368
12. EPA	64	921	46	
13. EXECUTIVE OFFICE OF THE PRESIDENT	30	91	41	162
14. EX/IM BANK	2	4	24	30
15. FCA			1	1
16. FCC	16	40	10	66
17. FCSC				
18. FEMA	3	10	10	23
19. FERC (Included with DOE)				
20. FHLBB	1	1	1	3
21. FMC	7	26	26	59
22. FRS	10	10	10	30
23. GSA	49	124	42	215
24. HEW	4	142	142	288
25. HUD	2			2
26. ICC				
27. INTERIOR	200	150	150	500
28. JUSTICE (all personnel authorized)	50000			50000
29. LABOR	300	900	200	
30. MMC		2	2	4
31. NASA	92	3214	157	
32. NCUA				
33. NRC	34			34
34. NSF		14		14

AGENCY	TOP SECRET	SECRET	CONFIDENTIAL	TOTAL
35. NTSB	1	1	-	2
36. OPIC	NO REPORT SUBMITTED TO ISOO			
37. OPM	2			2
38. SBA	800	800	800	2400
39. SEC	50	50	50	150
40. SSS	2			2
41. STATE	155			155
42. TREASURY	5	3	3	11
43. TVA	25	60	3	88
44. USDA	10	100	300	410
45. USICA				0
46. USITC				0
47. USPS		1		1
48. VA	51	1230		1281
GRANT TOTALS -----	110,693	97,287	32,945	240,925
PER CENT -----	45.94%	40.38%	13.68%	

Agencies reported that 1137 guides have been developed and promulgated throughout the executive branch. It should be made clear, however, that 1045 of these are DOD guides and the rest consist of those prepared by only 12 agencies.

CIA action to develop guides deserves special note. Work was begun long before the effective date of the Order, so that on December 1, 1978, four comprehensive guides had been printed and distributed for use within the agency. Use of the guides was evident in all CIA components visited by ISOO representatives. Seven agencies have still not prepared any guides. While agencies are encouraged to prepare unclassified guides to facilitate their dissemination and use, this is precluded in certain instances by the sensitive nature of the information covered in the guide. For example, of the current 1137 classification guides, 17 are classified Top Secret, 155 are Secret and 217 are Confidential.

During inspections, ISOO analysts routinely review guides, and in some instances run audit trails on documents classified through the utilization of guides to determine if they have been properly classified. ISOO experience with the use of classification guides indicates that in many cases they are misunderstood by those who must use them. In many cases, broad reference to the guide itself is cited as the basis for classification without reference to specific sections or paragraphs of the Guide. In some cases questioned, the derivative classifier could not identify for the ISOO analyst the authority within the Guide for the assigned classification. These are typical problems that can only be resolved through extensive education and training.

Those agencies that have developed experience in the use of classification guides such as DOD, DOE, NRC and CIA find that the guides contribute significantly to the success of their programs. The fact that the guide specifies the classification level to be applied to cited categories of information and the duration of classification should result in uniformity in both the classification and declassification of like information.

ISOO will actively monitor the development and use of classification guides during FY 80. Those agencies and Departments that have no experience in their use will require counseling and assistance in order to comply with the mandate of the Order. The Department of Defense is currently preparing a comprehensive booklet on the development and use of classification guides. This should prove extremely valuable to all agencies of the executive branch.

d. Original Classification Decisions. For purposes of statistical reporting, agencies were requested to report the number of decisions to originally classify information both by classification level and duration of classification. Agencies reported that during the five-month period May - September 1979, 3,118 original Top Secret decisions, 102,332 original Secret decisions and 290,204 original Confidential decisions were made. Thus, a grand total of 395,654 original decisions were reported for executive branch agencies during the test period. Analysis of classification assignments shows that only .79 percent of all original classification decisions were assigned Top Secret classification, 26% were assigned Secret classification, and 73% were assigned Confidential. These figures compare favorably with percentage assignments reported in the 1977 ICRC report and give encouragement that under the new system nearly three-fourths of the information being originally classified is being assigned to the lowest classification category. (See Exhibits 5 and 6).

Regarding assigned durations of classification, reported results show that approximately 33 percent of all original decisions were assigned declassification or review dates of six years or less and 67 percent were assigned declassification or review dates ranging from over 6 years to 20 years.

Under E.O. 12065 the duration of classification is determined by the continued sensitivity of the information rather than level of classification assigned as was the case under previous executive orders. Therefore, it is not possible to compare the percentages attained in 1979 with previous years. Rather, the 1979 statistics will serve as a base upon which to gauge future progress in retaining classification for the minimum time consistent with national security needs. Results of the inspections indicate that some agencies are erroneously marking documents as original actions when in fact they are derivative actions. For example, it is the opinion of ISOO analysts that the vast majority of the classification actions of the Department of Justice (DOJ) are derivative in nature rather than original. Since reported statistics show that DOJ accounted for nearly 34 percent of all original actions, these improper priorities have a negative impact on determining the actual status of six-year declassification or review. Had the DOJ figures been discounted, results would have shown that nearly half of all original classification decisions were designated for declassification or review in six years or less. ISOO emphasis on this aspect of the program should result in more accurate and improved statistics in the future.

DOCUMENT CLASSIFICATION DECISIONS
(Original Top Secret, Secret, and Confidential)

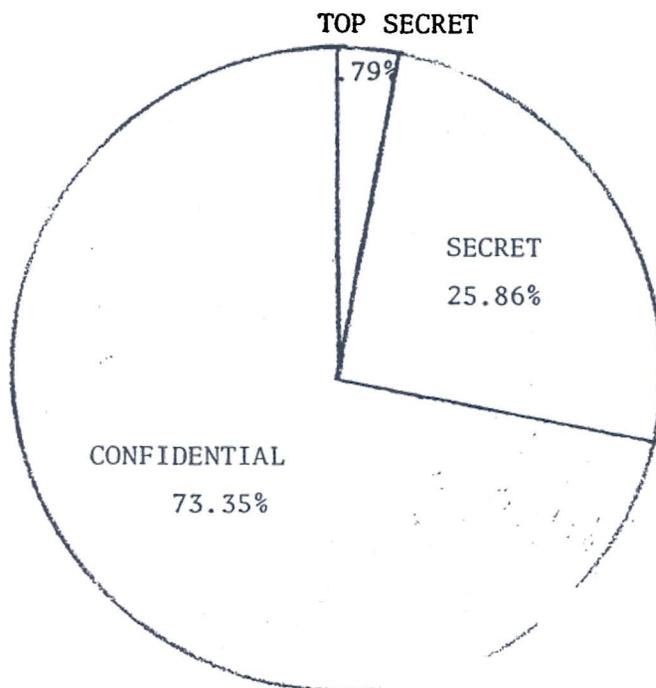
AGENCY	ORIGINAL TOP SECRET			ORIGINAL SECRET			ORIGINAL CONFIDENTIAL		
	0-6	6-20	Total	0-6	6-20	TOTAL	0-6	6-20	TOTAL
1. ACDA		8	8	102	154	256	120	8	128
2. AID (1)				8	-	8	81		81
3. CIA		1421	1421	1312	17903	19215	5946	58541	64487
4. COMMERCE				28	-	28	2625	1	2626
5. DOD		973	973	7220	13010	20230	67118	24438	91556
6. DOE (2)		10	10	45	47	92	240	31	271
7. DOT				-	-	-	-	-	-
8. EXECUTIVE OFFICE OF THE PRESIDENT	29	31	60	353	52	405	724	9	733
9. EX/IM BANK				-	-	-	1	-	1
10. FEMA	1		1	23	-	23	60	-	60
11. GSA				-	-	-	-	-	-
12. JUSTICE	4	603	607	95	51784	51879	532	80441	80973
13. NASA				3	-	3	10	-	10
14. NRC				-	-	-	-	-	-
15. OPIC (3)									
16. STATE	2	36	38	3786	6376	10162	39243	9368	48611
17. TREASURY				16	1	17	292	1	293
USICA				4	10	14	346	28	374
GRAND TOTALS	36	3082	3118	9937	99337	102332	117338	172,866	290204
PER CENT	32.95	0-6 years	.79	Top Secret					
	67.05	6-20 years	25.86	Secret					
			73.35	Confidential					

Because State and AID have no special markings to differentiate between original and derivative actions, the totals for original are high and those for derivative low.

- (2) Does not include RD and FRD (Secret 33,300; Confidential 93,100).
(3) No report submitted.

	0-6 years	6+-20 years	TOTAL
TS	36	3,082	3,118
S	12,995	89,337	102,332
C	117,318	172,886	290,204
GRAND TOTALS -----			395,654

EXHIBIT NO. 6
DOCUMENT CLASSIFICATION DECISIONS
(Original Top Secret, Secret, and Confidential)



KEY:

Number of original Top Secret decisions-----	3,118
Number of original Secret decisions-----	102,332
Number of original Confidential decisions-----	209,204

Reviews of documents by ISOO analysts and interviews with classifiers reveal that in some instances the previous linkage between assigned classification levels and duration of classification persists. In addition, some classifiers are setting a classification duration of 6 years or 20 years with no apparent regard for options to set declassification dates earlier than those periods. A unique problem of concern to the ISOO is the practice in some agencies of setting a date for review at 6 years, rather than a date for automatic declassification. While this practice does not appear to be in violation of the letter of the Order, it promises to be the basis for an administrative review burden a few years hence that agencies will have neither the time nor resources to meet.

While the Oversight Office is pleased with the first steps agencies have taken in the initial period of implementation in retaining classification for minimum periods, it is at the same time concerned that some agencies are assigning automatic six-year declassification dates without due regard for the impact of declassification of that information on the national security at the end of this short period.

Some classifiers have informed the ISOO analysts that they are hard pressed to live up to the spirit of the Order which emphasizes openness through relatively short periods of classification. Characteristics of the information with which they deal makes it difficult, if not impossible, to generate documents that can be declassified in 6 years or less. For example, the sensitivity of information concerning a device or weapons system could conceivably require continued protection for 40 or 50 years or more. Examples were provided to the analysts of devices/systems that were close to 20 years old before they were put into production.

Information regarding the number of documents whose classification was extended beyond 20 years by agency heads is not included in this report because of a variance in reporting by agencies which precludes the formulation of meaningful statistics.

e. Derivative Classification. Prior to E.O. 12065 agencies were not required to report derivative classifications separately. Some agencies experienced difficulty in compiling statistics in this area and are attempting to develop improved techniques to resolve the problem before the

deadline for the next report. Agencies submitted estimates on derivative classification in accordance with ISOO reporting requirements. Of the 28 agencies that derivatively classified (during the reporting period), 4 informed the ISOO that they had no way of differentiating between original and derivative decisions and therefore submitted no estimates.

Reported results show that the other 24 executive branch agencies estimated that 5,782,910 instances of derivative classification occurred during the five-month test period. Of this total, 3 percent were classified at the Top Secret level, 26 percent at the Secret level, and 71 percent at the Confidential level. It should be made clear that these derivative actions are not new decisions but merely the application of markings to material that contains information previously classified by an original classification authority.

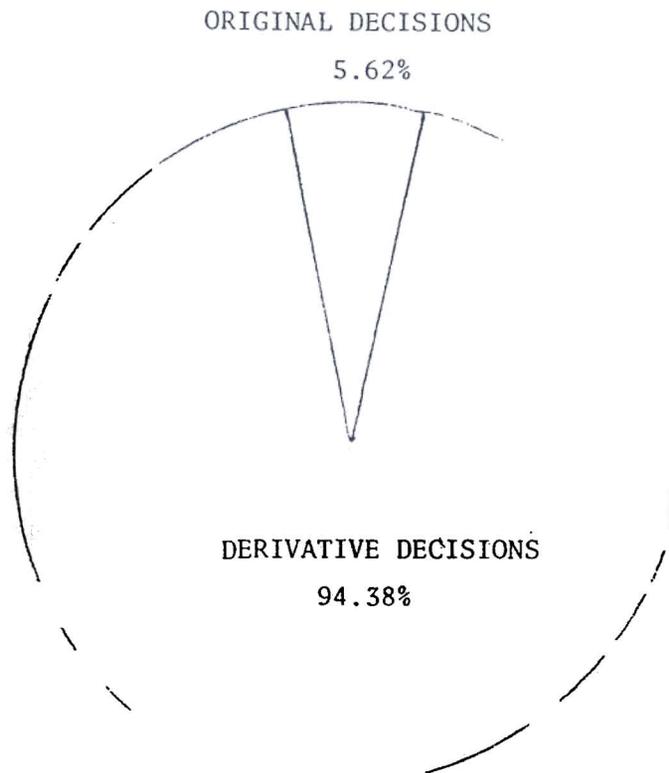
f. Original Versus Derivative Classification. While no firm figure was available in the past regarding the ratio of original to derivative classification, the ISOO had made an assumption that derivative classification constituted approximately 95 percent of all classification. Overall plans for monitorship of the program were developed to place maximum emphasis on the derivative classification aspects. The results of this initial reporting period show that derivative classification does constitute 94 percent of all classification, thus confirming the ISOO assumption. Future monitorship actions of both the agencies and the ISOO must be geared to control both the quantity and quality of derivative classification. (See Exhibit 7).

EXHIBIT NO. 7

CLASSIFICATION

DOCUMENT CLASSIFICATION DECISIONS

(Original versus Derivative)



KEY:

Number of original classification decisions ----- 5.62%

Number of derivative classification decisions ----- 94.38%

NOTE: The above percentages are based upon those reporting derivative classification decisions. AID, Commerce, State, and USICA did not report derivative decisions; therefore, their original classification decisions were subtracted in order to provide the above comparisons.

g. Total Classification Decisions. The combined totals of original and derivative classification show that executive branch agencies classified or marked for classification in 6,178,564 instances during the five-month test period. It is interesting to note that this figure exceeds the totals reported for the entire year of 1977 by nearly 50 percent. It is the contention of the ISOO that this increase does not indicate an escalation in classification on the part of executive branch agencies but rather a significant improvement in the receipt by the program oversight body of statistics that more accurately reflect the actual volume of information being classified.

h. Marking. The Order and the ISOO Directive require all paper documents to bear standard markings regarding their origin, classification, and duration of classification. The most common deficiency disclosed by ISOO inspections has been the absence of designators to indicate the classification of portions of a document, including the subject.

Portion marking is mandatory under the provisions of Executive Order 12065. Except for DOD elements, it is a new requirement and some lack of compliance can be expected until personnel are sufficiently trained and become accustomed to the portion marking habit.

Because of the wide distribution of Department of State information, laxity in portion marking by that agency has contributed to overclassification and unnecessary classification. ISOO has taken the position with the Department of State that improved education and direction is needed to cause State's classifiers to follow the mandate of the Order. Following the ISOO inspection of the U.S. Embassy in London, review of cables generated by the Embassy showed a significant increase in the use of portion marking. The ISOO and State are currently working together to achieve similar improvements in other State facilities.

Section 1-504 of E.O. 12065 grants the Director of the ISOO the authority to grant or revoke waivers to the portion marking requirement for specified classes of documents or information. Since the effective date of the Order, the Director has granted waivers in only three instances:

(1) On January 19, 1979, the Director granted the Department of Defense a conditional waiver from the portion marking requirements on the Secretary of Defense's 1979 posture statement. The waiver was conditioned on the fact that

the statement would not be used as a basis for derivative classification until such time as an addendum was prepared indicating the classification of all items in the posture statement.

(2) On August 3, 1979, a waiver from the portion marking requirements was granted for one item of intelligence information prepared by the CIA. Requests for waivers on five other items were denied.

(3) On August 30, 1979, the Director granted a waiver from portion marking requirements for nuclear propulsion information (NPI). The waiver was limited to NPI generated by and disseminated between specifically-named offices. The waiver also provided that all NPI will, in addition to other markings prescribed in E.O. 12065, be marked to prohibit the use of the information as a basis for derivative classification. Only the approved classification guide may serve as a basis for the derivative classification of NPI.

The ISOO Directive authorizes the use of abbreviations and/or codes on documents transmitted electrically. One major agency (the State Department) has adopted a system for indicating the duration of classification in terms almost identical to abbreviations used under the previous Order. Because the systems for designating duration under the two Orders are different, there has been some confusion on the part of recipients in other agencies. The problem is compounded by the fact that the same agency regulation prescribing the abbreviations is also applicable to three other agencies and that the use of the abbreviations is appearing on documents other than those transmitted electrically. The ISOO has pointed out these problems and violations to the agency and is continuing its efforts to resolve the problem. As an interim measure, the agency has expressed willingness to brief those agencies that have indicated that the use of the agency's abbreviations is causing them problems or confusion.

Marking problems concerning the authority for classification were noted in a limited number of agencies. These included instances of classification without authority and also identification of an original classifier when in fact classification was derived from an existing classified document or classification guide.

In some agencies drafts of working papers are passed outside the agency with overall classification markings but without other required markings. Frequently these documents become the basis for derivative documents and their lack of marking contributes to unnecessary classification and overclassification. To combat this problem some agencies have placed severe limitations on the dissemination of such documents until they are fully marked.

Other marking errors noted during the course of the ISOO inspections included:

The continued use of markings prescribed by E.O. 11652.

Failure to record the reason and authority for extension on information whose classification is authorized for periods in excess of 6 years.

The use of unauthorized terms such as "agency," "sensitive," or "conference" in conjunction with the three classification designations prescribed by the Order.

The marking errors cited in this section represent those most commonly found during the ISOO's conduct of 123 formal inspections. They are not all inclusive nor should they be interpreted as those occurring in all executive branch agencies. On the contrary, considering the volume of information classified, the relative newness of the program, and the constant turn-over of personnel in sensitive positions, agencies are making a reasonable effort to meet the marking requirements of the Order and the Directive.

3. Declassification

a. General.

Major changes in the information security program brought about by Executive Order 12065 dealt with the importance placed on declassification. For the first time, the Order mandates that agencies place emphasis on declassification comparable to that afforded to classification. The maximum period for retaining classification on national security information was changed from 30 years to 20 years. The Order requires that information be declassified as early as the national security will permit. Also mandated is

the requirement that agencies develop and promulgate guidelines for the systematic review of information as it becomes 20 years old. Further, agency heads are required by the ISOO Directive to designate experienced personnel to assist the Archivist of the United States in the review of United States and foreign government information.

A significant change not found in previous orders is the requirement that information extended by the head of an agency beyond 20 years be systematically reviewed at ten-year intervals. On October 1, 1979, the Director of ISOO issued a waiver from the 10-year review requirement for certain categories of information. These categories deal primarily with intelligence sources and methods and cryptography. The waiver was developed in close coordination with the CIA and was coordinated with the other major agencies of the Executive Branch. The waiver provides that after the 20-year review required by the Order, the next review for information falling into the specified categories will be conducted after an additional 30 years and thereafter at 10-year intervals.

The Order changed the very basis by which declassification is accomplished; instead of basing the term of classification on the classification level, the Order requires that declassification now be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event.

As mentioned earlier, the Order included for the first time a specific balancing test. This provision provides in certain cases for the balancing of the public's interest in knowing information against the need to provide it continued security protection. Reported results indicate that this provision was applied in some instances during the year. Moreover, no complaints were registered by the public with the ISOO concerning the application of this provision.

The provisions whereby a member of the public may request a mandatory review of national security information has been continued. This is particularly significant since it is the only avenue for possible public access to classified Presidential material.

b Declassification Actions

While actions to accelerate declassification have barely commenced, some agencies of the executive branch have taken positive steps to carry out their responsibilities.

The Central Intelligence Agency has established a new component to conduct systematic review of its records. This component is staffed with individuals with a mix of disciplines and backgrounds. Internal procedures have been developed for the unit and an ADP system has been developed to record review actions taken by the organization. During the period May 1 - September 30, 1979, 2.7 cubic feet (5,736 pages) of material was declassified. Projected on an annual basis, the agency took declassification action on approximately 3% of the estimated volume of 20-year-old material to be reviewed by December 1, 1988. It is anticipated that the percentage of completion will increase as the systematic review unit and agency personnel attain increased proficiency in all aspects of the systematic review function.

In November 1978 the Department of State instituted a major reorganization of its procedures for handling declassification and release of documents including documents requested under E.O. 12065, the FOIA, and Privacy Act provisions. The reorganization moved the Department from a highly decentralized approach to a two-fold centralized structure.

Under the reorganization, administrative processing of individual requests for declassification and all record keeping was assigned to the Central Records division of the Department. For review of all classified documents, the Department set up a new unit: the Classification/Declassification Center (A/CDC), which includes 2 offices, the Office of Systematic Review (CDC/SR), and the Office of Mandatory Review (CDC/MR). Both offices are under full-time Directors and are staffed by 75 retired senior Foreign Service Officers, having specific and complementary expertise in different areas of foreign affairs, who work part-time and alternate between the two offices as the work requires. In addition to these two offices, there is a small policy staff attached to the Deputy Assistant Secretary's office.

The Office of Systematic Review reviews Department material at 20/30 years, reviewing a sample of between 5% and 10% of the total documentation for a given period. On the basis of this sample, which is selected by the Office of the Historian (PA/HO), CDC/SR drafts guidelines to be applied by the

Archives for the declassification of the remaining material. In the course of this review CDC/SR also determines whether documents selected by PA/HO for inclusion in the Foreign Relations of the U.S. may be declassified. The office has actually begun reviewing records for the period 1955 through 1957. Departmental action has been completed to transfer 1950-1954 records to the National Archives. This amounts to approximately 17 million pages of classified material. The Department has also started identifying significant records and scheduling time for systematic review and eventual transfer to the National Archives. It has requested that all State posts survey their holdings for documents subject to scheduling. The Department of State anticipates achieving review at the 20-year mark by 1985.

The Department of Energy has instructed each field office to prepare a plan for the systematic review of documents. The plan provides for the identification of documents for systematic review, review of the documents by qualified individuals, declassification where appropriate, referral to the Secretary of Energy for extension if necessary, and reporting and record keeping functions.

The Department of Defense issued a single systematic review guideline applicable to the entire Department. During the period covered by this report, major DOD activities accomplished the following:

- The Organization of the Joint Chiefs of Staff reviewed 171,500 pages and declassified 169,630 or 98.9 percent.
- The Department of the Air Force reviewed 1,863,000 pages and declassified 1,372,500 or 73.7 percent.
- The Department of the Army reviewed 534,000 pages and declassified 507,300 or 95 percent.
- The Department of the Navy reviewed 908,333 pages and declassified 682,000 or 75 percent.
- The National Security Agency reviewed 500,000 pages and declassified 134,126 or 26.8 percent. Material declassified as a result of this program was primarily communications intelligence derived from World War II German and Japanese communications -- material of significant interest to historians.

To summarize the Department of Defense's efforts in systematic review and declassification, more than 3,977,000 pages of classified material were reviewed of which 72 percent were declassified.

Throughout 1979 the greatest part of declassification effort in the National Archives was devoted to the re-review of nearly two million pages of documents withdrawn between 1972 and 1979 in accordance with the provisions of E.O. 11652. About 1.6 million of these pages were declassified and replaced in their proper file location as a direct result of these efforts. Over half a million pages of records over 20 years old were reviewed on behalf of individual researcher requests. Thirteen million pages of 20-year-old records were systematically reviewed for declassification under the provisions of E.O. 12065 during the year. Among the major records reviewed during 1979 were:

Records of the Army's Chief of Engineers (1917-42), Quartermaster General (1914-61), Surgeon General (1917-46), Far East Command reports (1945-48).

Records of various Naval Operating Forces (1941-59) and certain Naval Districts and Shore Establishments (1917-43).

Records of the Allied Control Council for Italy (1943-47), the Allied Commission for Austria (1945-47), and portions of the files of the Office of Military Government for Germany (1943-49).

Central Files of the Selective Service System (1940-47).

Records of the Foreign Economic Administration (1941-45).

More than 60 man-years were devoted to declassification review work by the National Archives in 1979. Congress has authorized an increase which will more than double the effort in 1980. With this increase, it is expected that over 30 million pages of records over 20 years old will be systematically reviewed for declassification and that the remaining documents withdrawn under E.O. 11652 will be re-reviewed.

C. Mandatory Review Requests and Appeals

The Order requires that each agency establish a procedure to handle requests from a member of the public, a government employee or an agency to review information for declassification. The ISOO has ensured that such provisions were included in each agency regulation that it reviewed. In

addition, mandatory review procedures and progress is included as an inspection item during ISOO reviews.

Agencies reported to the ISOO that 936 new requests were received under the provisions of E.O. 12065. This is an addition to the 1,283 unresolved cases carried forward from 1978. Of the cases acted upon during the year, 55 percent were declassified in whole, 28 percent were declassified in part, and classification was retained on 17 percent. While these figures indicate that agencies declassified a large percentage of the information requested, the ISOO is concerned that 1,233 cases remained unresolved at the end of the reporting period.

The Order also requires each agency to establish procedures to act within 30 days on all appeals from denials of requests for declassification. Under E.O. 12065 only 30 new appeals were received by the agencies. Sixty-eight appeal cases were carried forward from 1978. Of the appeals acted upon, 20 percent were declassified entirely, 55 percent were declassified in part, and classification was retained on 25 percent. There were 48 unresolved cases at the end of the reporting period.

D. Safeguards

Analysis of ISOO inspections indicates that agency personnel are generally more knowledgeable of safeguarding procedures than other aspects of the program. However, there is still a lack of compliance with certain basic requirements in some agencies. For example, in a few agencies, responsibility for the accounting of Top Secret documents was not clearly established, records of access were not maintained, and annual inventories were either not conducted or were not adequate.

Copying machines abound in most agencies. Although agency personnel are aware of the security hazards involved in using copies, improved mechanical or procedural methods are needed to limit or control reproduction of material.

In some agencies, combinations to locks on security containers were found not to have been changed at the intervals prescribed by the ISOO Directive and, combinations were not afforded the same level of protection as the contents of the container. In some cases, custodians were not aware of how many individuals knew the combination and often times, persons without requisite security clearance set combinations, thus effectively giving them access to classified

material. Some agencies were storing classified information in containers which did not appear to meet the standards for such containers established by the General Services Administration and in a few cases, storage containers were obviously inadequate. There were also indications in a few agencies that classified material was being destroyed in a manner that did not preclude unauthorized access.

Two agencies requested and received an ISOO waiver from a part of their annual Top Secret inventory requirement prescribed in Section IV-E of the ISOO Directive:

- On July 20, 1979, ISOO issued a waiver of the annual inventory requirements for Top Secret material stored in the Relocation and Reconstitution (R&R) Section, Declassification and Archival Branch, Document Division, Joint Secretariat, Organization of the Joint Chiefs of Staff. It was determined that much of the material was duplicative of other records and physical safeguards were adequate to meet the requirements of the Order and Directive.
- On September 12, 1979, ISOO issued a waiver of the annual Top Secret inventory requirements for sensitive cryptologic information in the National Security Agency/Central Security Service (NSA/CSS). A review of the facility confirmed that the information for which the waiver was sought is acquired, stored and accessed through automated systems rather than hard copy. Controls over information is adequate to meet the standards of the Order and Directive. In issuing the waiver, it was made clear that the waiver did not extend to collateral Top Secret information received by NSA/CSS.

In both cases of waiver issuance, the agencies and the sites where the Top Secret material was stored, were inspected by the Director and the Deputy Director of ISOO.

Reported results by Executive Branch agencies indicated that the current Top Secret inventory is 1,365,751.

In a few rare instances it was found that employees having access to classified information were not cleared through proper investigation. Generally, the opposite condition existed -- personnel were cleared in numbers and at a level which appeared to exceed needs. Some agencies have a blanket requirement

that all personnel employed be cleared for Top Secret, even though not all personnel are given access to information at that level or any level. Only a few agencies appeared to be effectively monitoring the granting of clearances based on actual need for access. It appears that there is widespread lack of understanding concerning the relationships among (i) investigative requirements, (ii) position sensitivity, and (iii) the granting of a clearance. As a result, investigative funds may be being wasted and personnel may be exposed to national security information for which they have no need-to-know.

A number of agencies were holding classified material which was either obsolete (with respect to content) or obviously excess to their foreseeable needs. Internal drafts and working papers comprised a significant percentage of the total. This condition, which complicated the accounting, control, and storage of classified information, appeared to result from the lack of an effective records management program in the agency -- or at least the ineffective operation of such a program with respect to classified records. The problem of excess holdings stems to some degree from a more general problem of a lack of control over classified holdings. For example, in most agencies control and accountability is decentralized to a very low echelon in the hierarchy, related classified and unclassified material is usually filed together, and in many instances classified records are overlooked in scheduling agency records for disposition.

E. Education and Training

As has already been alluded to elsewhere in this report, the most effective means by which to insure that the provisions of E.O. 12065 are being implemented is through effective agency self-oversight. There are many variables which insure effective self-oversight including top management support, but the key to program success revolves around a good agency education and training program. The President emphasized training when issuing the Order:

" . . . Each agency that handles classified information should take care to insure that its personnel understand and follow the new procedures."

While both the Order and the Directive allow for flexibility on the specifics of agency training programs, the Order requires agency heads to "familiarize" those of their personnel who have access to classified information with the provisions of the Order and implementing directives.

As might be expected, for those agencies that had no previous experience with a formal information security program, analysis shows that training is a major problem area. It was less of a problem in agencies with classification authority.

In general, agency training programs:

- 1) Tend to emphasize safeguards to the exclusion of the classification (including marking)/declassification process;
- 2) Usually do not include special training for those with classification/declassification authority; and,
- 3) Frequently do not extend training to all personnel who have been granted access.

Some agencies devoted considerable resources and showed ingenuity in their training programs. For example, DOD and State Department offer through their departmental education systems formal courses in information security: DOD through the Defense Industrial Security Institute; State through the Foreign Service Institute. CIA took notable initiative to familiarize all agency personnel with the Order and Directive. Initial orientation, consisting of an excellent tape-slide presentation with a question/answer period, was presented in 52 sessions prior to the effective date of the Order. In addition, information security packages have been included in various internal agency training programs.

DOE has an excellent training program which uses a variety of media. Training is conducted on a scheduled basis; in addition, periodic refresher courses are offered.

As one aspect of their training program, NRC published a "Reference Notebook for NRC Authorized Classifiers" which was distributed to all authorized classifiers. Inspections by ISOO indicated this document is widely used and is very effective.

During 1979 the Information Security Oversight Office conducted formal training sessions on the provisions of the Order and also worked with individual agencies on regulations and training program development. Formal ISOO training began at the outset of the Order (January 31, 1979) with a one-day seminar on the mechanics of the Order. A year-end symposium was held on November 28, 1979, to look at specific features of the Order, which ISOO felt were of importance. The symposium concentrated on derivative classification, classification guides, and congressional and industrial perception of the Order. The November symposium was attended by over 400 security professionals from within the executive branch. Reaction to the day's activities was positive and there was a desire by some agencies that follow-up training programs be conducted by the ISOO staff for individual agency security personnel.

In addition to formal training programs, the ISOO Director and Deputy Director visited the agencies personally to meet senior officials and to brief security officials on the Order as well as to receive agency mission briefings. This seemed to be advantageous for both the agencies and the ISOO since it provided the opportunity to clarify those provisions of the Order which caused confusion; i.e., regulation development, systematic review guidelines. This was particularly true with those agencies new to the program.

The Director appeared before the National Classification Management Society's Annual meeting in May of 1979 to deliver the keynote address. He also appeared before agency training symposiums throughout the year. All of these appearances provided the Director excellent opportunities to discuss the Order and the status of its implementation. In all cases, ISOO presentations were well received.

1980 will be a year of fine tuning and continued training will play an important role in assuring that each of the executive agencies covered under the Order are in compliance.

RECOMMENDATIONS

Based on the experiences of 1979, ISOO feels there are 6 areas where specific improvements are needed to insure successful E.O. 12065 implementation. Those recommendations listed below are meant to give the President an indication of where program support is needed and where his active participation will enhance the ISOO's efforts in achieving the goals of the Order.

Recommendation #1: Training Needs -- The key to resolving many of the problem areas brought out by this Report is the active support of agency management for the development of comprehensive information security training programs.

Recommendation #2: Access -- Support is needed to reinforce the cooperative spirit ISOO has sought in 1979 to work with agencies where they have experienced access difficulties so as to arrive at an accommodation. Access to classified information is the key to the ability of ISOO to meet its oversight responsibilities.

Recommendation #3: Agency Support -- Agency heads should review their information security program to determine whether additional personnel and resources are needed to effectively implement the Order. If so, adequate budget planning should be undertaken.

Recommendation #4: Declassification Review -- In order to insure that the executive branch is to achieve the 10-year requirement of meeting the 20-year declassification review target as mandated by Section 3-405 of the Order, agencies should concentrate their efforts on the declassification aspects of the Order during FY 80.

Recommendation #5: Development of Classification Guides -- Support is needed to insure that agencies will put maximum emphasis in 1980 on the development of classification guides and will conduct training in their use as a part of the agency's overall information security program.

Recommendation #6: Data Collection -- Support is needed to insure that agencies collect the statistical data requested by the ISOO to insure an accurate accounting of an agency's information security program. In addition, increased monitorship is needed by the agencies to insure that the data collected accurately reflects the activities of their information security program and that such data is submitted in accordance with ISOO instructions.