Annual Report to the President

1980-1981

Information Security Oversight Office

General Services Administration
Information Security Oversight Office
Washington, DC 20405

28 SEP 1981

The President
The White House
Washington, DC 20500

Dear Mr. President:

I am pleased to submit the 1980-81 Report to the President of the Information Security Oversight Office.

Under Executive Order 12065, effective December 1, 1978, this Office oversees the information security program throughout the executive branch. Receiving its policy direction from the National Security Council, this Office has monitored the first several years of a program in which the prior administration stressed openness in government as the cornerstone of information security. The information security system embodied in E.O. 12065 reflects that emphasis.

Many persons within the Government's information security community have felt that the existing system downplays the critical importance of protecting national security information. Your administration has given credence to efforts to remedy the perceived imbalance between openness and security concerns. As a result, considerable efforts are now in progress to design an easier to understand information security system that serves this purpose. I hope to recommend this new system to you in the very near future.

Respectfully,

Steven Garfinkel

STEVEN GARFINKEL
Director

INFORMATION SECURITY OVERSIGHT OFFICE

CURRENT ACTIVITIES

- COORDINATING THE EXECUTIVE BRANCH REVIEW AND POSSIBLE REVISION OF EXECUTIVE ORDER 12065
- DEVELOPING INFORMATION SECURITY BRIEFINGS FOR THE WHITE HOUSE AND OTHER EXECUTIVE BRANCH ACTIVITIES
- CONDUCTING COMPLIANCE INSPECTIONS OF EXECUTIVE BRANCH AGENCIES AND CONTRACTORS
- CONDUCTING FOUR IN-HOUSE SPECIAL STUDIES OF INFORMATION SECURITY TOPICS WHICH IMPACT ON COST AVOIDANCE ASPECTS OF THE SYSTEM
- GATHERING AND ANALYZING EXECUTIVE BRANCH-WIDE STATISTICS ABOUT INFORMATION SECURITY
- SPONSORING SEMINARS AND SYMPOSIA
- ACTING ON PUBLIC APPEALS, COMPLAINTS AND SUGGESTIONS
- ACTING ON AGENCY REQUESTS FOR WAIVERS FROM CERTAIN PROVISIONS OF THE EXECUTIVE ORDER
- PARTICIPATING IN GOVERNMENT AND PROFESSIONAL SOCIETY TRAINING PROGRAMS
- PLANNING AN INFORMATION SECURITY TRAINING CLEARINGHOUSE
- PROVIDING DAY-TO-DAY LIAISON WITH EXECUTIVE BRANCH AGENCIES ON INFORMATION SECURITY MATTERS
- COORDINATING EXECUTIVE BRANCH RESPONSES TO GENERAL ACCOUNTING OFFICE REPORTS ON INFORMATION SECURITY
- CHAIRING MEETINGS OF THE INTERAGENCY INFORMATION SECURITY COMMITTEE
- ACTING ON AGENCY REQUEST FOR ORIGINAL CLASSIFICATION AUTHORITY

INFORMATION SECURITY OVERSIGHT OFFICE

AUTHORITIES AND RESPONSIBILITIES OF

THE DIRECTOR UNDER EXECUTIVE ORDER 12065

- OVERSEEING EXECUTIVE BRANCH-WIDE AGENCY ACTIONS TO ENSURE COMPLIANCE WITH E.O. 12065 AND ISOO IMPLEMENTING DIRECTIVE # 1.
- CONSIDERING AND TAKING ACTION ON SUGGESTIONS AND COMPLAINTS FROM PERSONS WITHIN OR OUTSIDE THE GOVERNMENT WITH RESPECT TO THE ADMINISTRATION OF THE PROGRAM.
- DEVELOPING, IN CONSULTATION WITH THE AGENCIES, AND PROMULGATING, SUBJECT TO THE APPROVAL OF THE NATIONAL SECURITY COUNCIL, IMPLEMENTING DIRECTIVES WHICH ARE BINDING ON ALL AGENCIES.
- REPORTING ANNUALLY TO THE PRESIDENT ON THE IMPLEMENTATION OF THE ORDER.
- REQUIRING INFORMATION DETERMINED TO BE CLASSIFIED IN VIOLATION OF THE ORDER TO BE DECLASSIFIED.
- REVIEWING AGENCIES' IMPLEMENTING REGULATIONS AND GUIDELINES FOR SYSTEMATIC DECLASSIFICATION REVIEW.
- EXERCISING TOP SECRET CLASSIFICATION AUTHORITY.
- REVIEWING REQUESTS FROM AGENCIES FOR ORIGINAL CLASSIFICATION AUTHORITY.
- CONDUCTING ONSITE REVIEWS OF AGENCY INFORMATION SECURITY PROGRAMS.
- REQUIRING OF EACH AGENCY INFORMATION, REPORTS, AND COOPERATION NECESSARY TO FULFILL THE DIRECTOR'S RESPONSIBILITIES.
- CHAIRING AN INTERAGENCY INFORMATION SECURITY COMMITTEE.
- CONSIDERING, GRANTING, AND/OR REVOKING WAIVERS OF ADMINISTRATIVE REQUIREMENTS OF THE ORDER.
- APPROVING SPECIAL PROCEDURES ESTABLISHED BY THE SECRETARY OF DEFENSE AND THE DIRECTOR, CENTRAL INTELLIGENCE AGENCY, REGARDING THE REVIEW AND DECLASSIFICATION OF CRYPTOLOGIC INFORMATION AND INTELLIGENCE SOURCES AND METHODS.

- HEARING AND ACTING UPON APPEALS FROM THE DENIAL OF REQUESTS FOR DECLASSIFICATION OF PRESIDENTIAL MATERIAL.

- HAVING NON-DELEGABLE ACCESS TO ACCOUNTINGS OF ALL AGENCY SPECIAL ACCESS PROGRAMS.

INFORMATION SECURITY OVERSIGHT OFFICE

1. Agency missions, programs, and authorities.

The Information Security Oversight Office (ISOO) was established pursuant to Executive Order 12065 on December 1, 1978. It is responsible for monitoring the information security programs of all executive branch agencies which create or handle national security information and for reporting annually to the President on the status of the program and agency implementation of the Order. There are over 100 executive branch agencies which create or handle national security information, although this activity is concentrated in the Departments of Defense, State, Justice and Energy and the Central Intelligence Agency. ISOO's purpose is, through effective oversight, to bring about improved protection for information essential to our national security while facilitating access by the American public to that information that does not require protection.

2. Basic organization and functions.

ISOO is a small organization consisting of 15 persons. Its functions include: (a) conducting in-depth onsite compliance inspections of over 100 executive branch agencies or major components of those agencies; (b) gathering and analyzing statistical data to obtain information upon which to evaluate compliance; (c) sponsoring information security education and training programs; (d) developing and promulgating directives implementing the Order; (e) reviewing agency regulations, classification guides and guidelines for systematic review of information for declassification; (f) taking action on suggestions and complaints from persons within or outside the Government with respect to the administration of the program, including complaints about the classification of documents; and (g) conducting special studies related to the functioning and improvement of the information security program.

3. Budgetary and financial information.

ISOO funding is included as a part of the budget of the National Archives and Records Service. The ISOO budget for FY 1981 is $563,000.

4. Personnel policies and administration.

ISOO's status as an agency is somewhat unusual. While administratively a part of the General Services Administration, it receives its policy direction from the National Security Council. In practice it operates semi-autonomously. The Director of ISOO occupies a career SES position and is appointed to that position by the Administrator of General Services, subject to the approval of the President. The Administrator of General Services also has, by the provisions of Executive Order 12065, the authority to appoint the staff of ISOO, although this function is ordinarily delegated to the Director.

5. Significant interagency relationships.

A close and continuing relationship exists between ISOO and senior personnel of the more than 100 agencies or major components monitored by ISOO. This involves coordination primarily with agency heads or with the senior officials designated by the agency heads to be responsible for the agency information security program. Each agency is also served by an ISOO staff member in a liaison role, which greatly facilitates the conduct of routine communication.

6. Significant intergovernmental relationships.

Since a segment of the program may involve security agreements with various foreign nations, ISOO is required on occasion to coordinate and hold discussions with representatives of those countries. These meetings are arranged by and coordinated with the Department of State.

7. Legislative processes, including legislative clearance requirements.

ISOO is established and functions under Executive order rather than statute, based on the premise that constitutionally only the President may regulate the executive branch's information security program. In the past, however, ISOO has worked closely with several congressional committees or subcommittees, including the House Subcommittee on Government Information and Individual Rights and the House Subcommittee on Administrative Practice and Procedure. ISOO and its predecessor organization, the Interagency Classification Review Committee, have been actively involved in commenting on and presenting testimony during hearings on proposed legislation for codifying the information security system. At one time, as many as nine proposed bills to this end were before the Congress. With the promulgation of E.O. 12065, legislative initiatives in this area have decreased significantly.

MONITORING COMPLIANCE

ISOO bases its evaluation of agency compliance and progress primarily on the results of (i) onsite compliance inspections, and (ii) analysis of statistical data submitted by all agencies which create or handle classified information.

ONSITE INSPECTIONS

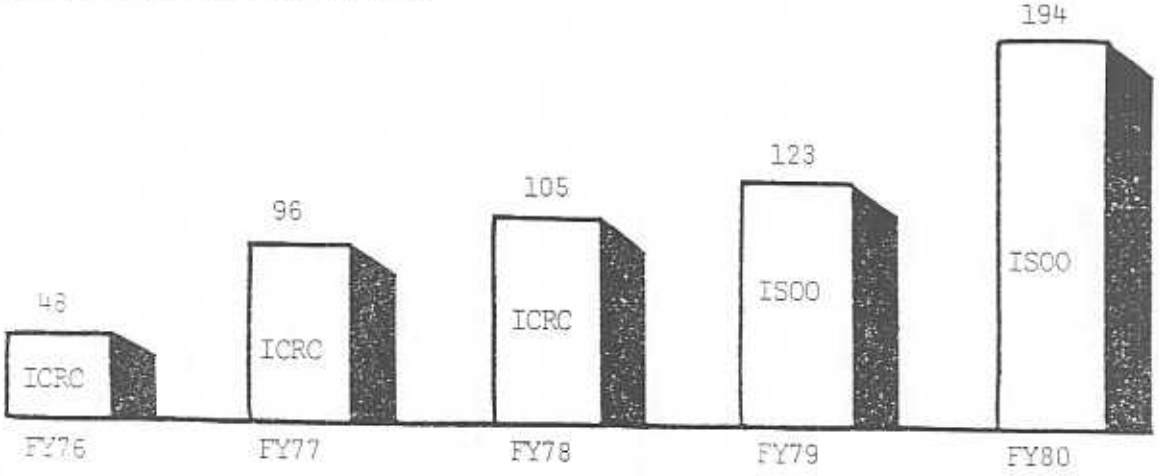
Within the United States and throughout the world, there are tens of thousands of facilities which create or handle classified information. With a full-time staff that presently totals 15 persons, ISOO can realistically hope to inspect only a fraction of 1 percent of these activities in any given year. Fortunately, an ISOO inspection of every facility is not only impossible, it is also unnecessary. By motivating senior agency officials and security personnel to police their own programs and by strategically directing ISOO's staff to selective points throughout the program environment, ISOO can successfully monitor the executive branch-wide system with limited resources.

ISOO's mode of operation places maximum emphasis on the conduct of inspections in those agencies that are the major classifiers and devotes minimal time and resources to those agencies that are only custodians of classified information and are not involved in the classification process. During FY 80, ISOO analysts conducted 194 in-depth inspections for which formal reports were submitted to the inspected agencies. Of these, over 50 percent involved an inspection of activities in the Departments of Defense, State, Energy, and Justice, and the Central Intelligence Agency—the major classifying activities of the Government. The number of inspections conducted in FY 80 exceeded by 57 percent the inspection activity of FY 79. In addition to formal inspections, the ISOO staff also conducted informal visits and follow-up reviews to previous inspections.

During the year ISOO also conducted a series of formal inspections outside the Washington metropolitan area. The areas visited included Atlanta, St. Louis, Norfolk, Philadelphia, and Boston. During each of these week-long trips, an ISOO analyst conducted a formal inspection of approximately six government activities. Included in most of these visits were inspections of government contractor facilities—a first for ISOO monitorship and an area that is receiving increased emphasis this fiscal year. Nine contractor facilities were inspected during FY 80.

The inspections covered the entire information security field including classification, downgrading, declassification, safeguarding, education and training and administrative requirements.

FORMAL INSPECTIONS BY THE OVERSIGHT ORGANIZATION

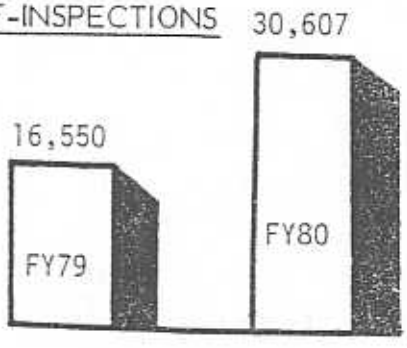


An essential element of each inspection was an examination of documents classified by the activity. This examination focused on such matters as proper classification, marking, declassification and control.

ISOO prepares and submits a report of each formal inspection. Each report includes both the findings of the ISOO analysts and recommendations to resolve problem areas or to achieve overall program improvement. These reports are sent to the senior agency official responsible for the program. Procedures adopted during FY 80, required agency officials to implement the recommendations and to notify ISOO of action taken within 60 days of receipt of the report. In the vast majority of cases, the officials took responsive action on these matters and notified ISOO as required. A reevaluation of the previously discovered problem areas and the remedial action taken were made a part of subsequent ISOO inspections.

The inspections conducted during FY 80 by ISOO and the agencies had a significant impact on identifying program weaknesses and achieving overall program improvement. The agencies conducted over 30,000 formal inspections of their own activities and in so doing, identified over 18,000 security infractions dealing with access, marking, transmission, storage, destruction and reproduction. This is an 87 percent increase in the number of formal inspections conducted when compared with FY 79 and a 114 percent increase in the number of detected infractions. The increase in the number of infractions appears attributable to the increase in the number and quality of inspections conducted rather than a degradation of the system.

AGENCY SELF-INSPECTIONS



STATISTICAL DATA COLLECTION

The collection and analysis of statistical data regarding information security program operations are an integral part of the oversight evaluative process. Over the years statistical data reporting requirements have been changed to more adequately meet the needs of the Oversight Office and the public for information regarding the program, to achieve cost reductions by eliminating items of minimal significance, and to facilitate the administrative burden on reporting agencies. In FY 80, ISOO significantly amended Standard Form 311—the single form used by agencies to report statistical data to the Oversight Office. This form provides ISOO information regarding:

- Classification authorities
- Classification decisions including declassification assignments
- Mandatory declassification review requests and appeals
- Systematic review for declassification
- Formal agency inspections and infractions discovered
- Top Secret inventories
- Declassification actions
- Security education and training
- Physical security actions
- Use of the balancing test
- Program management problems

Collection of data from a large universe can be very expensive and, in some cases, e.g., the Department of Defense, prohibitive. It is the opinion of ISOO that, except where specific agency information is required, satisfactory results can be obtained from statistical samples. ISOO accepts approved sampling in the larger agencies and has conducted its own sampling in connection with agency inspections to verify statistics provided by the respondents.

In providing the statistical data for FY 80, ISOO granted permission for sampling systems in the Departments of Defense, State, and Justice, and in the Central Intelligence Agency. All other agencies reported on an actual count basis. The Department of Defense sample was based on the results of an automated message system designed at a 95 percent accuracy rate. The reporting on classification actions other than messages was achieved by applying correlation factors based on an in-depth sampling conducted by DoD in FY 79. In addition, classification actions for the National Security Agency (NSA), to include all electrically forwarded product and administrative messages, were included for the first time. Failure to include NSA data had been a matter of concern by the General Accounting Office in a report on the program issued in 1980. The data submitted by the Department of Justice and the Central Intelligence Agency were based on a document by document count for a 1-week period and were projected to cover the entire reporting period. The Department of State statistics were taken from an automated system and correlation factors consistent with those determined by ISOO sampling were applied to determine the number of derivative classification actions over the year.

An analysis of the statistical data reported to ISOO by agencies for FY 80 indicates that respondents made concerted efforts to increase both the accuracy and validity of the reported data. ISOO received full cooperation from agencies in conducting its own statistical samples and was able to conduct such reviews on a random basis.

A definitive judgment on the effectiveness of agency implementation based on the results of program inspections and statistical data is not possible as yet; sufficient comparative data are still lacking. But progress achieved thus far has permitted the start of a foundation of an evaluative system that should be able to answer the questions in the future. This system will assist ISOO in determining the most effective direction for the program and the manner in which its limited resources should be allocated among various program components.

THE STATE OF THE PROGRAM

FY 80 was the first full fiscal year of operations for ISOO and, although conclusions based on data covering such a limited period are not absolute, it is possible to make some observations on the results.

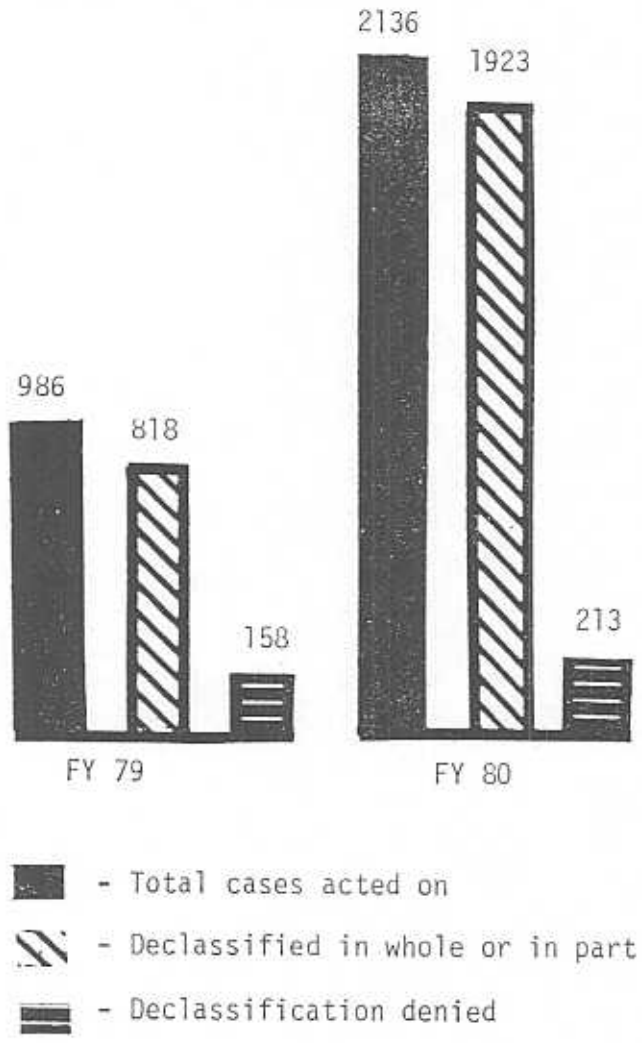
OPENNESS

ISOO has taken positive steps to achieve the openness initiatives in the Order. Internally, its operations have been conducted and recorded to minimize the number of classified documents within ISOO. Almost all documentary material within ISOO is available for inspection by the public upon request. Moreover, ISOO and executive branch agencies have taken action in a responsible and timely fashion on requests from the public for assistance or in instances where administrative conformance has been questioned. On numerous occasions during the year assistance was provided to the media, historians, faculty and students of academic institutions, and members of the public.

An area of progress over FY 79 involves agency actions taken in response to mandatory review requests from the public to review information for declassification. Despite substantial increases in the number of new requests received during FY 80, agencies acted on nearly 1150 more cases and declassified the information in whole or in part in 90 percent of the cases as compared with 83 percent in FY 79. The 10 percent denial-in-full rate is the lowest rate achieved since the monitorship program was begun in 1972. In the area of appeals from denials of mandatory review requests, the agencies further declassified in whole or in part in another 69 percent of the cases. Agencies reduced the backlog of unresolved appeal cases from 48 at the end of FY 79 to 29 at the end of FY 80.

On the negative side, at the end of FY 80 there were still over 1,200 unresolved initial requests. Moreover, in 46 percent of the cases acted upon during the year, action was not completed within the 60-day time-frame established by the Order.

MANDATORY REVIEW ACTIONS



Among selected activities by the agencies during FY 80 to enhance openness are the following:

National Security Council (NSC). Extensive efforts are underway in the NSC to update and reissue the listing of declassified NSC policy papers to provide another avenue for public access to declassified information. In addition, the NSC Director of Freedom of Information visited the Truman and Eisenhower Presidential Libraries to explore methods of expediting mandatory review procedures.

Department of Energy (DOE). DOE is in the process of screening and sanitizing all its records related to radiation health effects and the conduct of past U.S. nuclear testing. Copies of all relevant records will be made available to the public through a reading room and library arrangement at the DOE Nevada Operations Office.

Central Intelligence Agency (CIA). During the reporting period the National Archives and Records Service (NARS) accessioned some CIA records and others are under consideration. NARS has also been given a printout from the Agency's ADP system indicating the review decisions on a record group of finished intelligence, most of which was declassified. This will enable NARS to take the indicated action on its own copies, thus making the information available to the public.

Department of State (STATE). State has begun an experiment to test the effect of declassifying (but embargoing) Foreign Relations of the United States (FRUS) manuscripts six months in advance of the anticipated publication date in the expectation that this will considerably reduce the delay which has ensued in the past between clearance for and actual publication of FRUS volumes. State has also devised a system whereby scholars interested in Departmental records on a given country held by NARS may be given a computer printout listing the documents on that country declassified by State during its review of the material for the purpose of preparing systematic review guidelines. These documents are expected to provide scholars a tenfold increase in the number of pages as compared with FRUS compilations.

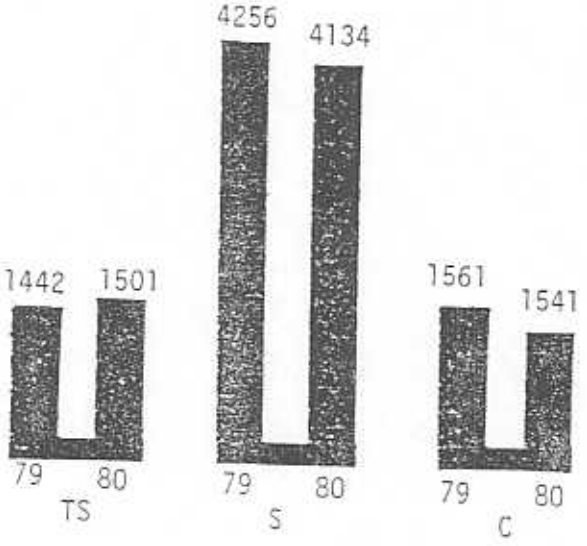
Agencies also initiated positive action during the year to establish systematic review programs. In all, over 90 million pages of previously classified information were reviewed for declassification. Of the 90 million pages reviewed, less than 2 percent had their classification extended beyond 20 years.

CLASSIFICATION

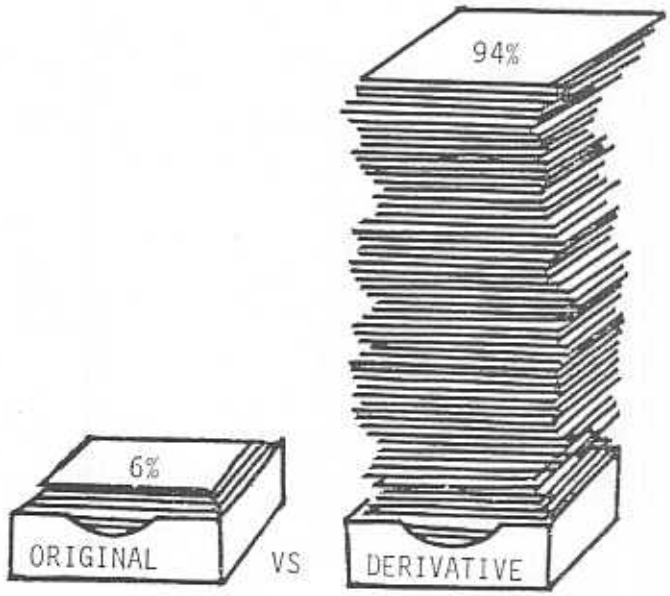
A. Classification Authorities. During FY 80, executive branch agencies continued the favorable trend of reducing original classification authorities. Overall authorities were reduced by 160 (2 percent). At the end of the reporting period there were only 1,501 persons in the entire executive branch authorized to make original Top Secret classification decisions, 4,134 designated as original Secret classification authorities, and 1,514 as Confidential authorities. Within the classification designation categories, there was a 1 percent increase in Top Secret authorities, and a 3 percent decrease in both Secret and Confidential authorities.

Overall, the distribution of authorities remained essentially the same as FY 79: 21 percent Top Secret, 58 percent Secret and 21 percent Confidential. An analysis of 1500 inspection reports indicates that minimal reduction can still be achieved in this area since approximately 6 percent of authorized original classifiers are not actively using that authority.

ORIGINAL CLASSIFICATION AUTHORITIES



The continued reduction of original classification authorities has a significant impact on the program, because originally classified information is the basis for derivatively classifying additional documents. Thus, a reduction in authorities has both an initial and accelerator effect in reducing classification activity. Reported statistics for FY 80 show that derivative classification again accounted for over 94 percent of all classification actions.



B. Classification Activity

During FY 80 executive branch agencies reported an approximate 10 percent increase in both original and derivative classification actions. A total of 16,058,764 actions were reported for the year as compared with 14,850,000 for FY 79. Of the total actions reported, 3 percent were assigned a Top Secret classification, 9 percent Secret and 68 percent Confidential. This is essentially the same ratio as that achieved in FY 79. While some of the increase in classification actions must be attributed to improved and more accurate reporting by the agencies and the inclusion of additional agencies in the universe such as the National Security Agency, most is believed to be the result of specific events which bear on national security. For example, during the year agency classification activity was influenced by the

change of government in Iran, the hostage situation, events in Afghanistan, the Middle East and other areas of the world. This clearly points out the impact of current events on the number of classification decisions and the difficulty of evaluating program improvement in this area because of the correlation.

Of the approximate 1 million original classification decisions made during FY 80, 33 percent were assigned declassification or review dates of 6 years or less. This is the same percentage obtained in FY 79.

ISOO's in-depth inspections indicate that, in general, agencies were in compliance with the provisions of the Order as they apply to classification. However, some specific areas were discovered that require added emphasis by agency security personnel. These areas are listed below. (Numbers in parentheses indicate the percentage of inspections in which these types of deficiencies were noted.)

- Incomplete or improper markings--(35%)
- Lack of portion marking—(26%)
- Failure to mark subjects—(18%)
- Marking derivative actions as original—(12%)
- No classification guides issued—(9%)
- Failure to update guides--(7%)
- Using unauthorized caveats—(14%)
- Failure to include TS approval on guides—(2%)
- Inconsistency in assigned classifications—(2%)
- Using obsolete stamps or markings--(13%)
- Classifying without authority--(4%)
- Failure to list multiple sources—(3%)
- Unnecessary classification—(5%)
- Failure to use cover sheets—(1%)

FY 80 was the first year in which formal ISOO inspections were conducted at Defense contractor facilities. The results of this initial examination indicated strong management support for the program and commendable accounting and safeguarding procedures. However, the General Accounting Office has cited recurring deficiencies in the area of classification guidance and the application of such guidance to documents. This is an area that requires additional emphasis by ISOO and budgeting and planning has been accomplished to permit increased ISOO inspections during FY 81.

DECLASSIFICATION

A. General. Fiscal Year 1980 brought an increase in the scope of the declassification program within the executive branch of government. More agencies instituted declassification projects and those with programs already in effect continued to improve their output in an attempt to reach the goal and requirement of the Order that information be systematically reviewed for declassification on the twentieth anniversary of its creation.

B. Systematic Review. During FY 80, the General Accounting Office (GAO) investigated the systematic review process. In a report published October 15, 1980, GAO recommended that the Executive order be revised to eliminate systematic review and to require that only records specifically requested or likely to be requested by the public be reviewed under the provisions of the Freedom of Information Act (FOIA) or the mandatory review provisions of the Order. GAO claimed that such action would result in substantial savings to the Government. ISOO responded to the GAO report on behalf of the executive branch stating that to eliminate systematic review, and to rely entirely on the FOIA and mandatory review would be a retraction of the government's commitment to openness and would leave large portions of government records unavailable for research. Further, ISOO pointed out that the increased use of and the high costs associated with processing under the FOIA and mandatory review would most likely make the system more costly and burdensome than at present.

Interestingly, the problem in the declassification field most often brought to ISOO's attention by the agencies has been the limited resources available to

accomplish mandatory review and declassification functions; this includes comments from the major classifying activities such as the National Security Council, the Central Intelligence Agency, and the Departments of Defense and Energy. The results of ISOO inspections have also shown a direct link between the lack of adequate resources and full and effective implementation of the Order.

C. Achievement of 20-year Review. The lack of sufficient resources has resulted in several activities informing the ISOO that they cannot meet the 1988 deadline for achieving 20-year review. For example, the National Security Council has stated that present budgetary limitations preclude their reaching the goal. The CIA anticipates that it will have only systematically reviewed 30 percent of its material by 1988. Other agencies such as the Department of Energy, Office of Management and Budget, National Aeronautics and Space Administration, International Communication Agency, Commerce and the Agency for International Development indicate that they cannot yet determine when or if they will reach the 20-year point. Seven activities, the Nuclear Regulatory Commission, Treasury, State, National Security Agency, Defense Intelligence Agency, Defense Investigative Service and the Office of the Secretary of Defense have indicated they will be in compliance with the 20-year rule between 1982 and 1988. Three activities, Interior, Agriculture and the Organization of the Joint Chiefs of Staff, have already achieved the 20-year goal.

A particularly critical problem exists within the National Archives and Records Service (NARS), which has the largest declassification program in the Government. NARS has indicated that the continuation of budgetary and personnel limitations during 1980 will preclude it from reaching the 20-year review goal.

ISOO considers the systematic review program and the problems associated with it to be a major priority subject. It is conducting an in-depth study on the subject during FY 81. If the result of the study shows that the requirements of the Order cannot be met, then consideration will be given to requesting the President to modify the Order.

D. Other Declassification Actions. During FY 80 executive branch agencies reviewed over 90 million pages for declassification purposes. Overall, nearly 24 million pages or 27 percent were declassified. However, some impressive declassification rates were achieved by individual agencies (Office of Micronesian Status Negotiations-92 percent, Office of Management and Budget-83 percent, Department of State-54 percent, International Communication Agency-52 percent, and the Department of Defense-98 percent, of nearly 6 million pages it reviewed). The lower 27 percent declassification rate can be attributed to the fact that NARS, the major reviewer of record series classified material, spent much of its time during the year re-reviewing records withdrawn during the 1972-1978 period in accordance with the new systematic review guidelines developed under Executive Order 12065.

Major records series reviewed by NARS for declassification during the year included the records of the Solid Fuels Administration for War (1950-1954); additional records of the War Relocation Authority 1942-1946); records of Naval Districts and Shore Establishments (1921-1953); National Headquarters Files of the Selective Service System; personal papers of General J. Lawton Collins as Special Ambassador to Vietnam (1954-1955); and the papers of General Lucius D. Clay as High Commissioner in Germany. In addition, the review of a number of very extensive and important files continued in 1980, e.g., intelligence files of the Army Assistant Chief of Staff for Intelligene, records of Foreign Service Posts of the Department of State (1948-54), records of the National Aeronautics and Space Administration and its predecessor agencies (1916-1958), and the U.S. Army Commands during the Korean War.

SAFEGUARDS

Problems in the safeguarding of classified information noted during ISOO inspections high-lighted the fact that security regulations do not guarantee protection. For example, in some agencies Top Secret material was not being inventoried; Top Secret control officers had not been appointed; and storage containers did not meet minimum standards. Further, classified documents in some instances were transferred between offices without proper document covers to identify them as classified; controls over reproduction of classified documents were lacking; and, in limited instances, obsolete security markings were still in use. In a few agencies, combinations to locks on security containers were not being changed at the intervals prescribed and names of the combination holders were not being recorded in one central location.

One of the most significant developments in improving the safeguarding of classified information was action taken by agencies to reduce material on-hand to the absolute minimum required for the accomplishment of the agencies' missions. In the wake of hostile actions against United States installations abroad, agencies with large holdings such as the Departments of Defense and State, and the Agency for International Development implemented accelerated retirement/destruction programs at both domestic and foreign locations.

Cost savings were a positive part of the 1980 information security safeguards program. Reductions in classified holdings resulted in a decreased need of security container requirements. Several agencies improved their procedures for granting security clearances. This reduces security investigation costs. One agency, for example, estimated they had reduced the number of critical-sensitive positions in the agency by over 700. This represents, in this one agency alone, possible future cost avoidances of over $1 million.

Other agencies reported to the ISOO that efforts to enhance safeguards included such programs as increased after-hours inspections; more stringent visitor control over entry to areas containing classified information; procurement of approved shredding machines to ensure destruction of obsolete material; more vigorous training/retraining programs; and improved procedures for reporting security infractions.

EDUCATION AND TRAINING

There is no question that effective education and training are the keystone to the success of the executive branch information security program. Continuous and improved training programs are essential because of the constantly changing personnel situation within the Government and because most personnel occupying security positions do so on an additional duty basis. For these reasons, ISOO and executive branch agencies devoted increased emphasis to education and training during FY 80. There is also no question that training played an ever-increasing role in maintaining a quality force of security professionals in those agencies where such positions are established. Moreover, there is ample evidence that effective training has improved not only skills, but also the motivation that, in turn, improves program implementation.

A. ISOO Findings. An analysis of a sample of over 100 ISOO inspections conducted during FY 80 indicated that improvement was needed in many security education areas. For example, ISOO surveys showed that 17 percent of inspected agencies had not established formal education programs; that 9 percent needed improved education programs that distinguished the difference between original and derivative classification; that 30 percent showed a need for improved training on marking; and that in 28 percent of the inspections, a need was identified for improved training on internal safeguarding procedures.

B. Agency Accomplishments. Noteworthy improvement was made in the development of improved security briefings and security

awareness programs across the executive branch. Typical examples of progressive action reported by some agencies include:

Agency for International Development (AID). In addition to holding weekly orientation sessions, AID held mandatory briefings during the week of September 22, 1980, in which 850 employees were instructed in all phases of document security--from preparation to destruction.

Department of Treasury. The Department conducted a comprehensive review of all Treasury education and training programs and, as a result, produced a major revision to its training program. This resulted in a package which is applicable Treasury-wide and which can be modified to meet the needs of individual components.

Nuclear Regulatory Commission (NRC). The NRC security poster program has won the First Place Award two years in a row at the American Society for Industrial Security (ASIS) annual national poster competition.

Department of State. The time alloted by State to the security briefing program has been doubled. In addition, the security office now provides a program of individual briefings for senior officers at the Deputy Assistant Secretary level and above, a group that includes ambassadors leaving for overseas posts.

Department of Defense (DoD). The DoD achieved major improvements in its security education program during the year primarily through increased emphasis on the subject by the Deputy Secretary of Defense (Policy Review). Significant security initiatives of a general nature include:

1. Development and dissemination of a guide for marking classified documents. This is a quality document that should result in improved DoD documentation marking and will also be useful to other executive branch agencies as a guide for preparing their own training aids.

2. Development and dissemination of a vastly improved DoD handbook on the preparation of security classification guidance. This again will prove of great value to other agencies with little or no experience in writing classification guides.

Significant gains were also made by DoD elements during the year. Examples include:

1. Defense Intelligence Agency (DIA). Three of the video tapes produced by the Agency and used in their security education program have won awards from the ASIS. The DIA has also developed a 30-minute slide and sound presentation which can be viewed by senior officials in their offices as their work schedule will permit. Because of its recognized excellence, much of the education material developed by the DIA has been used by numerous departments and agencies of the Government and the contractor community. The agency has also exchanged security education material with the Governments of Canada, Australia, and Japan.

2. Department of the Army (DA). In June 1980, DA sponsored its first Army Security Managers Conference in Washington, D. C. Because of its success, future conferences will be held every 18 months. The education program of the U.S. Army Europe and, in particular, its security managers course held in Vilseck, Germany, has received favorable comment during the year. Headquarters has also developed special security educational videocassettes which have been shown over the local Armed Forces TV network.

3. Department of the Navy. Navy's efforts have been directed primarily to educating the security manager so he or she will be able to train command personnel effectively; providing resources for use in the command security education program; and updating the level of instruction at Navy training facilities. Navy education programs currently include audio-visual briefings for Security Orientation, Classification and Declassification, Security for

Clerical Personnel, Personnel Security and Foreign Travel. The Navy has also revised its Security Manager Correspondence Course that is now required for all new security managers.

4. Department of the Air Force (USAF). During November 1979, the USAF held its third annual Air Force Worldwide Information Security Workshop. This brought together senior information security specialists from throughout the world. The USAF is continuing its efforts to establish a Civilian Specialist Career Management Program that will improve the quality of personnel and encourage young people to enter the security specialist field. The Department is also currently developing a series of instructional videotapes that will cover the key aspects of Executive Order 12065. These are aimed at the working level individual and will be suitable for self-study or group instruction.

C. ISOO Participation

During FY 80, ISOO analysts worked closely with agencies, particularly those minimally involved with classification, to assist them in developing or improving education programs. In addition, an evaluation of agency security training programs was made a part of all ISOO inspections.

The ISOO also participated in a number of agency or professional security society events during the year. For example, Senior ISOO officials spoke on numerous occasions at the request of agencies or other groups such as the National Classification Management Society. The Office also participated actively in the program of the Defense Industrial Security Institute, which continues to offer improved courses in information security and related areas.

Overall, FY 80 was a year in which agencies came to recognize shortfalls in their security education programs and took positive action to correct them.

OTHER AREAS FOR PROGRAM IMPROVEMENT

An area of considerable concern, as stated by the various agencies and offices monitored by ISOO, is the lack of sufficient resources to effectively implement the program--primarily inadequate funds allocated to information security programs. Usually, security duties are collateral and account for only a portion of an official's responsibilities. In such cases, time allocated to information security is, at best, minimal. Even agencies with full-time security personnel find that the enormity of the job often precludes accomplishing all of the goals of the Order with allocated resources. This lack of resources impacts primarily on the declassification review programs and security training within agencies. The subject of adequate resources is one that demands greatly increased attention by senior agency officials.

Another widely recognized problem deals with document marking. Many agencies, continue to express concern about the lack of uniformity in the markings applied throughout the executive branch. Of concern to these agencies is the fact that the variance in markings often makes it difficult to determine the source of original classification or the date or event for declassification or review. Similar concerns are expressed about the failure of some agencies to apply portion-marking to documents, a practice that compounds the problem of derivative classification and often provides a basis for under or overclassification. Agencies have expressed considerable concern that such practices could lead to inadequate protection for Foreign Government Information, particularly that dealing with intelligence sources and methods. In the most flagrant variations from the norm, ISOO has approached those agencies in an attempt to achieve greater standardization.

Another problem area involves the individuals designated as senior agency officials or

senior agency security managers. In some instances these officials do not have the authority to make decisions regarding the various aspects of the program within their agencies. This situation has the effect of limiting the level of security interest among such individuals; impeding the undertaking of security initiatives and, consequently, the effective implementation of the program; and greatly compounds the oversight problems faced by ISOO. Agency heads must ensure that individuals designated by them as responsible for the program have the latitude and authority to make the program work.

A significant problem that extends across the executive branch deals with information classified by the former emergency preparedness agencies and the current Federal Emergency Management Agency (FEMA). In conducting reviews and inspections, ISOO has discovered great quantities of classified information concerning emergency preparedness within agencies' files. Much of the material is outdated and obsolete. Further, there is often a lack of understanding among the holders of such information of which information is operative. Needless to say, this situation has serious impacts beyond the classification of the information. In an effort to remedy this stituation, ISOO has contacted FEMA and obtained the name of an official that agencies can contact to determine the currency of FEMA holdings. The senior officials of all agencies handling such material were provided this information by ISOO and were requested to undertake this review and updating of emergency management information.

The above action will also assist in the resolution of another prevalent problem—that of cleaning out and destroying obsolete material in files. In 24 percent of the ISOO inspections conducted during the year, ISOO analysts reported a need for a records clean-out program. Such programs result in increased security by reducing the chances of compromise of the destroyed information and by narrowing the available sources for the creation of derivative documents. This subject will continue to be a matter of interest during FY 81 inspections and should be given great attention by agency security and records management staffs.

FIRST HALF FY 81 ACTIVITIES

A. ISOO Liaison Role. Early in FY 81 ISOO began implementing certain measures designed to enhance the effectiveness and responsiveness of program oversight. One of these measures was the establishment of agency liaison roles for ISOO analysts for the purpose of furthering communication between agencies' information security staffs and ISOO. Under this system the designated analyst serves as the primary point of contact and provides assigned agencies with technical assistance and answers to inquiries on program related matters.

The agency liaison system has proven highly successful. It has provided for a freer and more direct means of communication as well as prompter handling of inquiries. It has also contributed to developing a pool of experts familiar with all aspects of agencies' information security programs, to include both strengths and weaknesses. This has facilitated the Director's decision-making by allowing him to utilize this pool of expertise.

The agency liaison concept complements a shift in oversight emphasis from a compliance to a systems oriented approach. This has resulted in more rounded oversight through the examination of the program on a government-wide perspective rather than on the basis of individual agencies' perceived problems.

B. ISOO Inspection Program. Through advanced planning, a formal schedule for ISOO reviews and inspections to be conducted in FY 81 was developed and coordinated with executive branch agencies This program has resulted in one and, in some cases, two visits to most agencies, including major subordinate elements. In addition, ISOO analysts have visited several defense contractors in California, Texas, and Washington. These were to:

- determine if the agency or contractor was complying with the Order and implementing directive;

- assess the effectiveness of the activity's information security program; and

- assist security program staffs by identifying the causes of problems, and to recommend remedial action.

The formal reviews and inspections have largely focused on four key sections of the Executive order—original classification, derivative classification, declassification and downgrading, and safeguarding.

Experience thus far in FY 81 inspections has shown that agencies are cooperating fully with ISOO and are providing ISOO analysts with necessary access to agency classified holdings and related records.

C. Security Education and Training. Consistent with the findings of ISOO inspections and reviews in FY 80, deliberative planning was conducted by ISOO to determine the best methods for oversight of security education and training during its FY 81 monitorship activities. These included increased concentration on the subject during scheduled visits to executive branch agencies, particularly in those smaller organizations that lack full-time security personnel; monitorship and review of courses conducted by the Defense Industrial Security Institute; attendance and participation in professional security organization presentations such as those conducted by the National Classification Management Society; monitorship of security briefings and training given by executive branch agencies; collection and evaluation of agency security education materials and training aids; and the development and presentation of standard briefings by ISOO itself to executive branch agencies.

In connection with the latter, ISOO developed two standard security briefings on the program. Both took the form of slide and tape presentations. The first was a short synthesis of the overall program and was designed to provide senior officials, particularly those without previous exposure to national security information, with an overview of the information program and their responsibilities under that program. This briefing was presented to the new National Security Council staff by ISOO. The second briefing developed by ISOO is a more detailed presentation covering the operational aspects of the program and is designed to meet the needs of agency security personnel, action officers, and administrative personnel. These briefings are available to agencies for use in their security education programs.

Initial evaluation of the increased emphasis on security education and training indicates that it is paying benefits in improving understanding of the program and better marking and protection of national security information. ISOO emphasis will continue on this subject throughout FY 81.

D. Annual ISOO Symposium. On November 19 and 20, 1980, ISOO sponsored a 2-day symposium. Selecting as its theme, "Information Security: Critical Perspectives," the program was designed to stimulate interest, thought and dialogue about the strengths and weaknesses of the executive branch information security program. In keeping with the theme of the program, speakers were selected who represented opposing views on the Order. Featured speakers on the first day's program were Seymour Hersh, formerly of the New York Times; John S. Warner, former General Counsel of the Central Intelligence Agency; Morton Halperin, Director of the Center for National Security Studies; Richard Hewlett, Senior Associate with History Associates, Inc., and former Chief Historian for the Department of Energy and its predecessor agencies; Salvatore Gallo, Jr., Security Manager, Orlando Division of Martin-Marietta Aerospace; and Robert Kimmitt, Staff Counsel, National Security Council. The second day of the program featured a round-table discussion by guest speakers centered around questions raised by

attendees. The Director, ISOO, served as moderator for both sessions.

Highlights of the symposium included stimulating discussions on the availability of classified information to the media and the attitude or responsibility of the media in handling such information; the significance and use of the "balancing test" provisions of the Order; and protection provided by the Order to foreign government information.

Approximately 700 people attended the 2-day program. The attendees included agency officials, security staff members, lawyers, Freedom of Information and public affairs personnel, and members of the general public. ISOO was encouraged by the response to the program and plans to sponsor additional programs in the future.

E. Special Studies. At the close of FY 80, ISOO critically examined its onsite inspection program to determine where to devote its limited resources. The examination showed that agencies were generally making significant progress in meeting the fundamental requirements of the Order. Thus, ISOO was able to limit emphasis on compliance inspections and to modify its oversight role by examining other areas of the program in need of attention.

In broadening its oversight role, ISOO has undertaken the conduct of four special studies. The focus of these studies is on the examination of particular aspects of the system from an executive branch-wide perspective. The topics were selected with a view toward examining cost avoidance aspects of the system; a related concern was to determine whether some of the requirements of the Order were contributing to effectiveness.

The four studies deal with the applicability of ADP technology to information security; the advantages and disadvantages of classification guides; the efficacy of systematic review of information for declassification; and, the practicality of standardizing information security forms. Each study is concerned with the possible adjustment of the system to make it more cost-effective.