TRANSMITTAL SLIP	DATE 23 APRIL 1986

TO:

ROOM NO.	BUILDING

REMARKS:

EXO/DDA Ben 23/4

ADDA

DDA

JOYCE

DDA Registry - File

FROM:

ROOM NO.	BUILDING	EXTENSION

FORM NO. REPLACES FORM 36-8 (47)

ROUTING AND TRANSMITTAL SLIP 23 APR 86

To: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. DIRECTOR OF INFORTATION SERVICES		
2.		
3.		
4.		
5.		

Action		File	Note and Return
Approval		For Clearance	Per Conversation
As Requested		For Correction	Prepare Reply
Circulate	XXXX	For Your Information	See Me
Comment		Investigate	Signature
Coordination		Justify	

REMARKS

708

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
EXO/DDA	Phone No.

STAT

STAT

5041-102 OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

Information Security Oversight Office
Washington, DC 20405

April 14, 1986

Dear Mr. Kerr:

I am pleased to provide you with a copy of the Information Security Oversight Office's (ISOO) "Annual Report to the President FY 1985." I also enclose a copy of the President's letter in response to the report, in which he expresses his appreciation and support for continued improvement in the Government's information security program.

This report contains information that should be provided to or shared with all those persons within your agency who are responsible for the creation or handling of national security information. ISOO's liaison to your agency is currently coordinating with your representatives to provide an adequate number of copies. We seek your full support in assuring that these copies are quickly and thoroughly distributed.

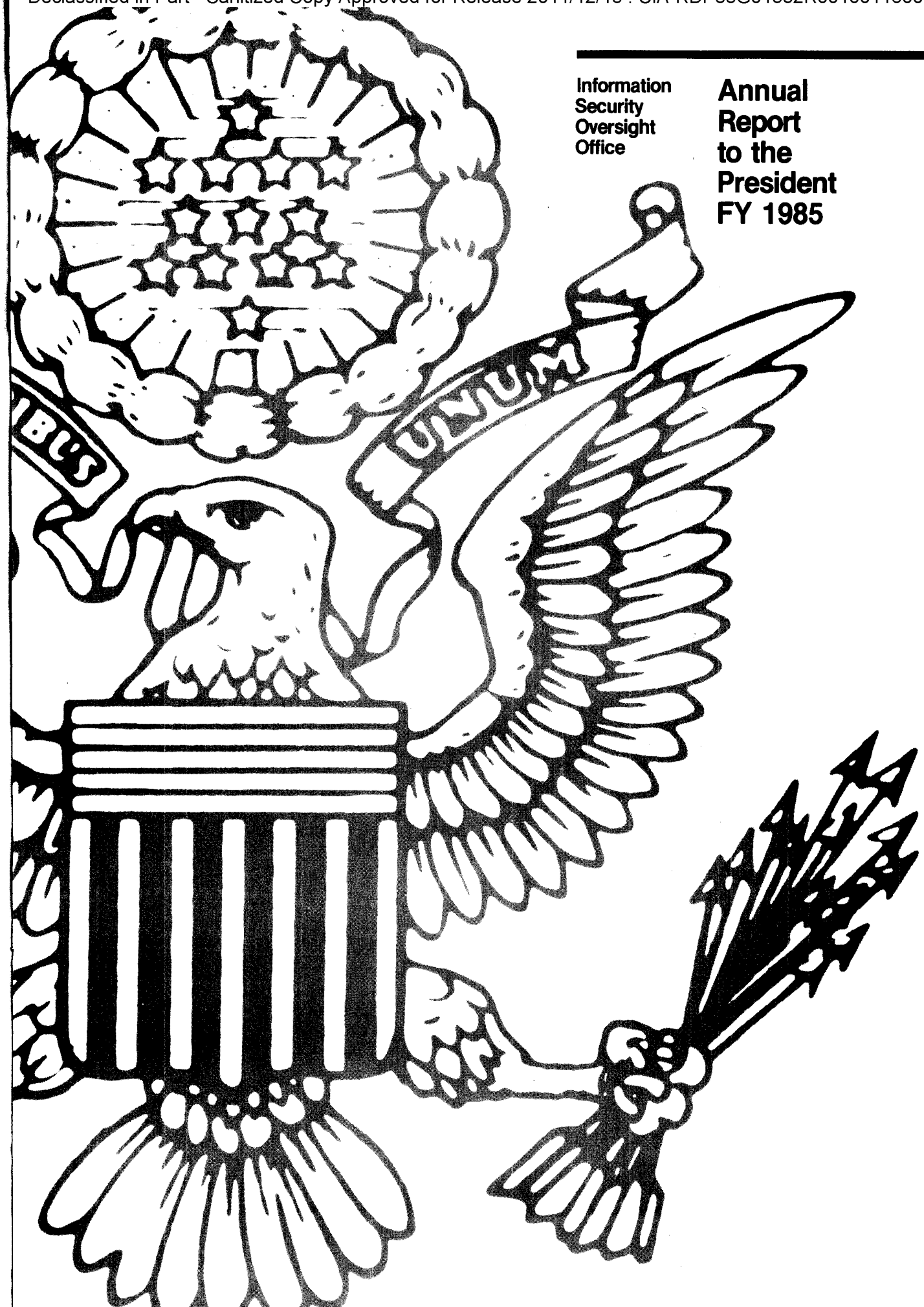
Sincerely,

Steven Garfinkel

Steven Garfinkel
Director

Mr. Richard J. Kerr
Deputy Director for Administration
Central Intelligence Agency
Washington, DC 20505

Enclosures



Information Security Oversight Office

Annual Report to the President FY 1985

THE WHITE HOUSE

WASHINGTON

April 11, 1986

Dear Mr. Garfinkel:

Thank you for your 1985 Annual Report on the status of the system we have established under Executive Order 12356 to protect national security information. I am pleased to note that the system continues to work well.

Your report noted the current efforts to improve the information security program which the National Security Council has since approved in principle. Your interagency committee is to be commended for these efforts. These initiatives, in conjunction with other security and counterintelligence initiatives, should assist in further strengthening the information security program.

Please accept my thanks for the outstanding work of your organization and the other dedicated personnel throughout the government who are working so hard on behalf of protecting our national security.

Sincerely,

Ronald Reagan

Mr. Steven Garfinkel
Director
Information Security Oversight
Office
18th and F Streets, N.W.
Washington, D.C. 20405

Information Security Oversight Office
Washington, DC 20405

March 24, 1986

Dear Mr. President:

I am pleased to submit the Information Security Oversight Office's (ISOO) 1985 Annual Report to the President.

Since you issued Executive Order 12356, "National Security Information," in 1982, the ISOO has regularly reported that the information security system established under it has functioned very well. That success continues.

Nevertheless, you have also recognized the need for ongoing efforts to improve the security classification program, seeking better protection for national security information without excessive classification. In 1985, the ISOO commenced an interagency effort to seek even further improvement in the information security program. The ISOO is now working to implement the proposed initiatives that resulted. These are discussed in greater detail in the Report.

Your support of the information security system has been constant and remains vital to its continued success. As we seek further improvement, we proceed with the knowledge of your continued interest.

Respectfully,

Steven Garfinkel
Director

The President
The White House
Washington, DC 20500

Table of Contents

Exhibits

Agency Acronyms or Abbreviations Used in this Report

ACDA	Arms Control and Disarmament Agency
AID	Agency for International Development
AIR FORCE	Department of the Air Force
ARMY	Department of the Army
BIB	Board for International Broadcasting
CEA	Council of Economic Advisers
CIA	Central Intelligence Agency
COMMERCE	Department of Commerce
DARPA	Defense Advanced Research Projects Agency
DCA	Defense Communications Agency
DCAA	Defense Contract Audit Agency
DIA	Defense Intelligence Agency
DIS	Defense Investigative Service
DLA	Defense Logistics Agency
DMA	Defense Mapping Agency
DNA	Defense Nuclear Agency
DoD	Department of Defense
DoE	Department of Energy
DoT	Department of Transportation
ED	Department of Education
EPA	Environmental Protection Agency
EXIMBANK	Export-Import Bank
FBI	Federal Bureau of Investigation
FCA	Farm Credit Administration
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FHLBB	Federal Home Loan Bank Board
FMC	Federal Maritime Commission
FRS	Federal Reserve System
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
ICC	Interstate Commerce Commission
ISOO	Information Security Oversight Office
INTERIOR	Department of the Interior
ITC	International Trade Commission
JUSTICE	Department of Justice
LABOR	Department of Labor
MMC	Marine Mammal Commission
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NAVY	Department of the Navy
NLRB	National Labor Relations Board
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
OA, EOP	Office of Administration, Executive Office of the President
OJCS	Organization of the Joint Chiefs of Staff
OMB	Office of Management and Budget
OMSN	Office for Micronesian Status Negotiations
OPIC	Overseas Private Investment Corporation
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
OSTP	Office of Science and Technology Policy
OVP	Office of the Vice President
PC	Peace Corps
PFIAB	President's Foreign Intelligence Advisory Board
PIOB	President's Intelligence Oversight Board
SBA	Small Business Administration
SEC	Securities and Exchange Commission
SSS	Selective Service System
STATE	Department of State
TREASURY	Department of the Treasury
TVA	Tennessee Valley Authority
USDA	Department of Agriculture
USIA	United States Information Agency
USPS	United States Postal Service
USTR	Office of the United States Trade Representative
VA	Veterans Administration

Summary of FY 1985 Program Activity

The FY 1985 Report to the President is the third to examine the information security program under E.O. 12356. The following data highlight ISOO's findings:

Classification Activities

- The number of original classification authorities rose slightly to 7,014.
- Original classification decisions decreased to a record low level of 830,641.
- By classification level, 3.9% of original classification decisions were "Top Secret," 35.6% were "Secret," and 60.5% were "Confidential."
- Under E.O. 12356, originally classified information has been marked for automatic declassification 34% of the time, in contrast to the estimated 10% rate under E.O. 12065.
- Derivative classification decisions rose 15% over FY '84, to 21,492,254.
- The total of all classification actions, 22,322,895, was a 14% increase over FY '84.

Declassification Activities

- Agencies received 4,037 new mandatory review requests.
- Agencies processed 3,621 cases, 18% fewer than in FY '84, but declassified in full 265,197 pages, 101,632 more than in FY '84, and declassified in part 47,920 additional pages.
- Agencies received 282 new mandatory review appeals.
- Agencies acted on 522 appeals, 23% more than in FY '84, and declassified additional information in whole or in part in 87% of the cases.
- Under the systematic review program, agencies declassified 8,107,047 pages of historically valuable records, 2.4 million pages fewer than in FY '84.

Inspections

- Agencies conducted 28,319 self-inspections, a slight increase over FY '84.
- Agencies reported 15,154 infractions, 21% fewer than in FY '84.

Information Security Oversight Office

The Information Security Program - FY 1985

Under Executive Order 12356, the Information Security Oversight Office (ISOO) is responsible for monitoring the information security programs of those executive branch activities that generate or handle national security information. Originally established by Executive Order 12065, ISOO continues to be the primary oversight organization in the system prescribed by President Reagan's Order of April 2, 1982. In this role, ISOO oversees the information security programs of approximately 65 departments, independent agencies and offices of the executive branch. E.O.12356 also requires the Director of ISOO to report annually to the President about the ongoing implementation of the Order's provisions. This Report summarizes Government-wide performance during FY 1985, the system's third year.

ISOO is located administratively in the General Services Administration but receives its policy direction from the National Security Council. The Administrator of General Services appoints the ISOO Director upon approval of the President. The ISOO Director appoints the staff, which numbers between 13-15 persons. For FY 1985, ISOO's budget was $660,000.

ISOO fulfills its assigned responsibilities under E.O.12356 in a variety of ways. First, it develops and issues implementing directives and instructions regarding the Order. Second, ISOO conducts on-site inspections or program reviews of agencies that generate or handle national security information. During FY 1985, ISOO also monitored agency implementation of the signing by all cleared employees of the Classified Information Nondisclosure Agreement, Standard Form 189, prescribed by National Security Decision Directive 84 (NSDD 84), as a condition of access to classified information. Appendix B, p. 27, reports on the status of implementation of this requirement by each agency. Third, ISOO gathers, analyzes and reports statistical data on agencies' programs. Fourth, it evaluates, develops or disseminates security education materials and programs. During FY 1985, ISOO held a symposium entitled "National Security Information: Different Perspectives," at which time Government and contractor employees, scholars and journalists heard varying views on the topic from a panel of experts assembled from the public and private sectors. Appendix C, p. 28, contains quotes highlighting the meeting. Fifth, ISOO receives and takes action on suggestions, complaints, disputes and appeals from persons inside or outside the Government on any aspect of the administration of the Order. In this area, ISOO serves as the final appellate authority for the mandatory declassification review of presidential materials. Sixth, it conducts special studies on identified or potential problem areas and on programs to improve the system. During FY 1985, the ISOO Director chaired an interagency effort to develop initiatives to improve the Government-wide information security system in five perceived problem areas: overclassification or unnecessary classification; the overdistribution of classified information; classification management; revitalization of the "need-to-know" principle; and unauthorized disclosures. These initiatives are discussed in greater detail in the narrative section, p. 19. Seventh, ISOO maintains continuous liaison with monitored agencies on all matters relating to the information security system. This Report is based upon program reviews and inspections conducted by the ISOO staff and the compilation and analysis of statistical data regarding each agency's program activity.

Program Reviews and Inspections

ISOO's program analysts serve as liaison to specific agencies to facilitate coordination and to provide for continuity of oversight operations. The analysts must stay abreast of relevant activities within each agency's information security program; coordinate with assigned agency counterparts on a continuing basis; and conduct formal inspections of the agency's program in accordance with a planned annual inspection schedule, which includes visits to selected field activities as well as offices in the Washington metropolitan area. ISOO also undertakes compliance reviews of selected contractor facilities as part of its inspection

program. Appendix D to this Report p. 30, lists those activities that ISOO has inspected during the period FY 1983-1985.

These on-site surveys encompass all aspects of the information security program, including classification, declassification, safeguarding, security education, and administration. The inspections always include detailed interviews with agency security personnel, classifiers, and handlers of national security information. To the extent possible, ISOO analysts review a sampling of classified information in the agency's inventory to examine the propriety of classification, the existence of necessary security markings and declassification instructions, and compliance with safeguarding procedures. ISOO analysts also monitor security training programs to determine if the agencies adequately inform personnel about classifying, declassifying, marking and safeguarding national security information. When weaknesses in an agency's program are identified, ISOO analysts recommend corrections, either on-the-spot or as part of a formal inspection report. Critical reports require immediate remedial attention by the agency prior to a follow-up inspection by ISOO. These inspections are a necessary means of identifying and resolving problem areas. They provide specific indicators of agency compliance or noncompliance with E.O. 12356 that are not apparent simply from the analysis of statistical data.

Statistical Reporting

To gather relevant statistical data regarding each agency's information security program, ISOO developed the Standard Form 311, which requires each agency to report annually the following information:

1. The number of original classification authorities;
2. the number of declassification authorities;
3. the number of original classification decisions, including the classification level of those decisions and the duration of classification;
4. the number of derivative classification decisions by classification level;
5. the number of requests received for mandatory review for declassification and agency actions in response to these requests in terms of cases, documents, and pages;
6. the number of pages of national security information reviewed during the year under systematic declassification procedures and the number declassified;
7. the number of formal self-inspections conducted by the agency; and
8. the number of security infractions detected by the agency within its own program.

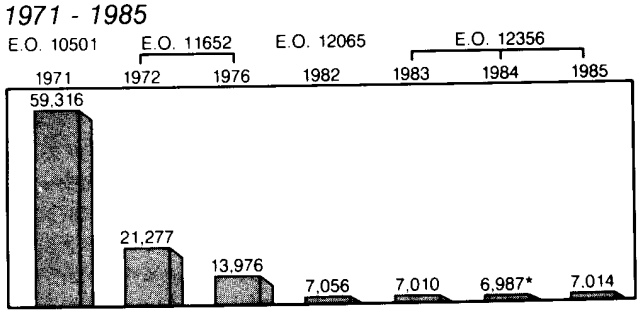
The statistics reflected in this Report cover the period October 1, 1984, through September 30, 1985. Some of the larger agency programs, including CIA and DoD, calculate their classification actions on the basis of sampling systems approved by ISOO. For FY 1985, DoD utilized two sampling methods in reporting its statistics to ISOO. The first is based on electronic message traffic only, and has been in use since ISOO began collecting these statistics. The second, which was begun this year, includes a wider range of document types, including memoranda and reports. For FY 1985, ISOO is using the data provided by the message traffic system in the body of the Report to allow for more accurate comparisons with previous years. In future reports ISOO intends to use the statistics provided by the new sampling method, because it is likely to produce more reliable figures. Appendix A, p. 24, describes the two sampling systems in greater detail, and contains the statistics reported by DoD using the new method.

Original Classification Authorities Up Slightly (Exhibits 1 and 2)

Original classification authorities are those individuals specifically authorized in the first instance to classify information in the interest of national security. These classifiers are designated in writing, either by the President or by other officials, primarily agency heads, named by the President. Limiting the number of original classifiers to the minimum necessary for efficient management is one way to control the volume of overall classification activity. ISOO encourages agencies to conduct regular surveys to ensure that the number of original authorities is in line with operational requirements.

ORIGINAL CLASSIFIERS **Exhibit 1**

1971 - 1985



* Totals Reported in FY 1984 ISOO Report Changed to Reflect Addition of 87 "Secret" Classifiers in DoD Not Previously Reported to ISOO

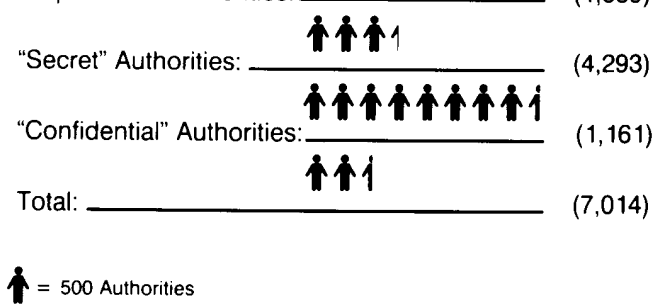
The number of executive branch employees authorized to classify originally has decreased significantly since 1972, when the figure was 59,316. In FY 1985, there were 7,014 individuals with original classification authority. This is slightly higher than the revised total of 6,987 reported in FY 1984, and approximates the 7,010 original classifiers registered in FY 1983. Responsibility for the higher figure during FY 1985, rests with three agencies that reported substantial increases. They are FEMA, up 13 (+325%), Treasury, up 26 (+30%) and State, up 136 (+8%). These numbers more than offset decreases at CIA, DoD and OSTP. The number of "Top Secret" authorities rose at the greatest rate (+3%), although "Confidential" authorities also increased by 1%. "Secret" authorities declined by 1%. During FY 1986, ISOO will press each agency that accounted for this year's increase, and others, to make a concerted effort to reduce the number of original classifiers, especially at the "Top Secret" level. ISOO is convinced that some designations of original classification authority continue to be based solely on the purported prestige that attaches to it. This is unacceptable because the only valid justification is the need of the official to exercise such authority in the performance of his or her employment responsibilities.

Original Classification Declines to Record Low Level (Exhibits 3 through 7)

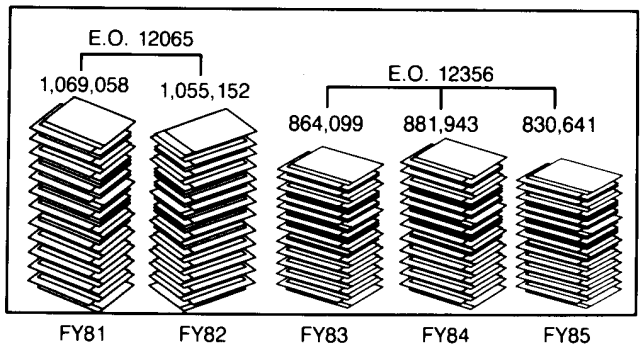
An original classification decision is an initial determination by an authorized official that information requires protection from unauthorized disclosure in the interest of national security. The determination is accompanied by the placement of required classification markings on the medium that contains the information. The number of original classification decisions is probably the most important statistic reported by ISOO each year because of its wide ranging impact on all aspects of the information security program.

In FY 1985, the number of original classification decisions decreased by 51,302 (-5.8%) to 830,641. This figure represents the lowest number of original actions reported since ISOO began collecting such statistics in FY 1979. The total is 21% lower than the 1,055,152 decisions reported in FY 1982, the last year under the previous Executive order.

NUMBER OF ORIGINAL CLASSIFIERS **Exhibit 2**

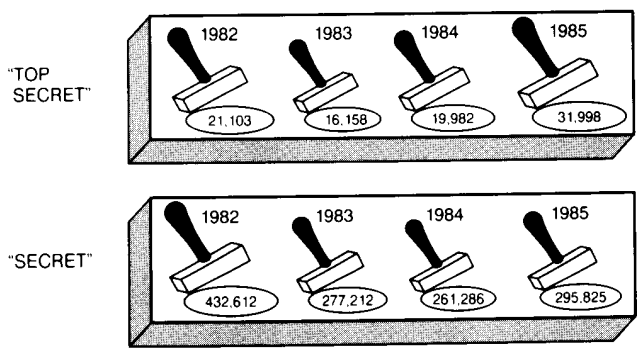


COMPARISON OF ORIGINAL CLASSIFICATION ACTIVITY **Exhibit 3**

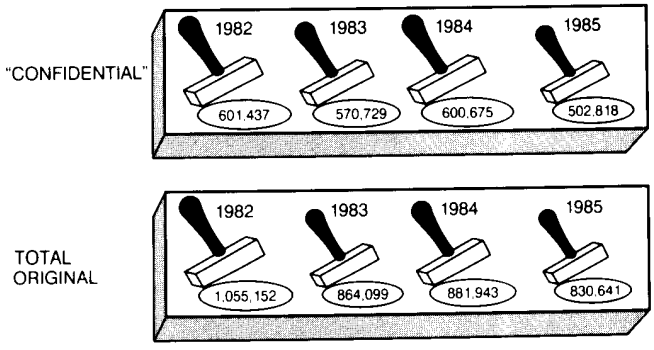


Despite the positive overall figure for FY 1985, ISOO notes that the number of original "Top Secret" actions increased substantially during the year. They rose by 12,016 (60.1%). "Secret" actions increased by 34,539 (13.2%). These numbers were offset by a dramatic decrease of 97,857 (-16.3%) in "Confidential" decisions. ISOO is concerned that a trend may be developing for agencies to classify at increasingly higher levels, and will be watching carefully to ensure that any continued movement in such a direction is justified.

ORIGINAL CLASSIFICATION DECISIONS **Exhibit 4**



ORIGINAL CLASSIFICATION DECISIONS **Exhibit 4**



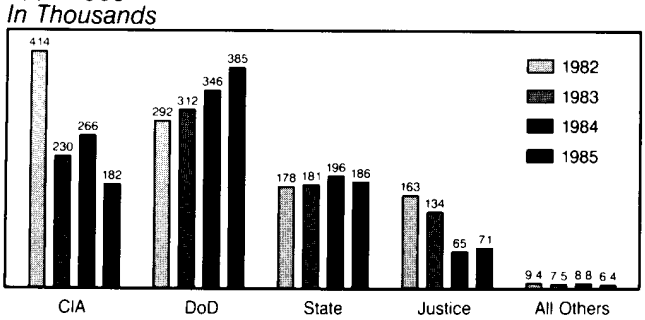
Four agencies classify originally more than 99% of the actions within the executive branch. Of these, DoD reported an increase of 39,577 (11%) and Justice a rise of 6,341 (10%). The CIA and State reported decreases of 32% and 5%, respectively. The decline of 84,500 actions by the CIA was the primary factor for the lower total figure in original classification decisions. A comparison of original classification decisions by agency for the period FY 1982-1985 shows a dramatic decrease by the CIA from a high figure of 413,521 reported in FY 1982, to this year's total of 181,688. Similarly, the numbers for Justice demonstrate a marked decline in original classification activity from FY 1982-FY 1985. The figures for State remained relatively constant during the period. The only major classifier to register increases each year is DoD, which reported 291,831 original decisions in FY 1982, and 385,496 in FY 1985, a 32% increase.

During FY 1985, 35% of the decisions specified a particular date or event for automatic declassification. This is 3% greater than the figure reported in FY 1984. The average of 34% under the current Executive order continues to be considerably better than the estimated 10% under the predecessor system.

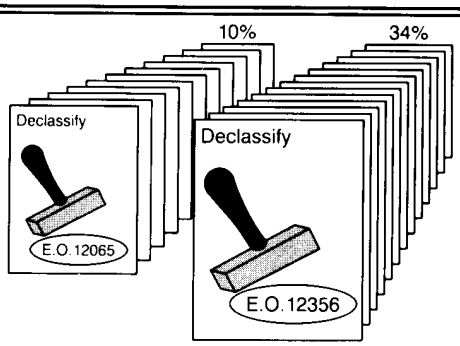
The DoD's automatic declassification rate remained an impressive 71% during FY 1985. However, at several other agencies the rate declined sharply from the percentages reported in FY 1984. They were the CIA (5% in FY 1984, to 1% in FY 1985), DoE (15% to 7%), State (12% to 8%), and Treasury (16% to 9%).

ORIGINAL CLASSIFICATION DECISIONS BY AGENCY **Exhibit 5**

1982-1985
In Thousands



ORIGINAL CLASSIFICATION DECISIONS SCHEDULED FOR AUTOMATIC DECLASSIFICATION **Exhibit 6**



During the course of its on-site inspections, ISOO analysts examine documents to determine the propriety of the classification and the proper use of markings. Frequently, analysts review items that could contain a specific date or event as the declassification instruction but instead bear the indefinite designation, "Originating Agency's Determination Required." Examples of documents that should contain a specific date or event as the declassification instruction are memoranda relating to itineraries abroad by U.S. officials or to this country by foreign dignitaries. This is an area in which further improvements are achievable. ISOO will continue to press agencies to use a date or event whenever possible.

Derivative Classification Continues to Rise (Exhibits 8 and 9)

Derivative classification is the act of incorporating, paraphrasing, restating or generating in new form classified source information. Information may be derivatively classified in two ways: (a) through the use of a source document, usually correspondence or publications generated by an original classification authority; or (b) through the use of a classification guide. Only executive branch or Government contractor employees with the appropriate security clearance who are required by their work to restate classified source information may classify derivatively.

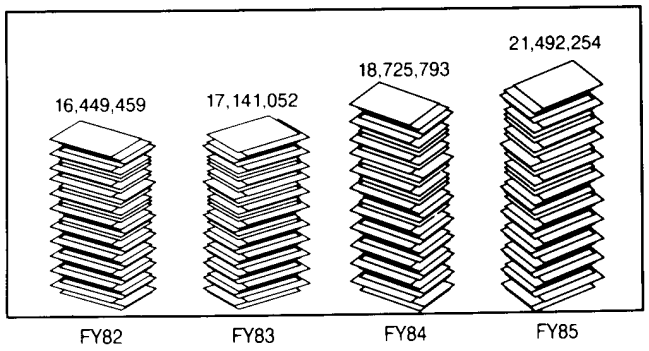
In FY 1985, executive branch agencies made 21,492,254 derivative classification decisions, a 14.8% increase over FY 1984. Of the total, 510,179 (2%) were classified at the "Top Secret" level, 6,539,860 (31%) at the "Secret" level, and 14,442,215 (67%) at the "Confidential" level. These figures represent an increase at each level, with the number of "Secret" actions rising the greatest at 18%. "Top Secret" and "Confidential" decisions increased 11% and 13%, respectively.

ORIGINAL CLASSIFICATION/ DECLASSIFICATION ASSIGNMENTS **Exhibit 7**

1985

Agency	% Assigned Date or Event for Declassification	% OADR (Must be Reviewed Before Declassification)	% "TS"	% "S"	% "C"
DoD	71%	29%	1%	18%	81%
CIA	1%	99%	14%	75%	11%
State	8%	92%	0.1%	20.9%	79%
Justice	0.4%	99.6%	4%	70%	26%
Treasury	9%	91%	0%	5%	95%
All Others	21%	79%	2%	25%	73%
Totals	35%	65%	4%	36%	60%

COMPARISON OF DERIVATIVE CLASSIFICATION ACTIVITY **Exhibit 8**



An examination of the data from FY 1982 through FY 1985 indicates that DoD and CIA account for nearly all of the derivative classification decisions. The figures for DoD show annual increases during the period from a low of 13,738,420 in FY 1982, to a high of 18,090,961 in FY 1985. The increase from FY 1984-1985, was 11% or an additional 1,826,923 derivative classification actions. The CIA had experienced declines in each year from FY 1982-1984. However, in FY 1985 it registered a 42% increase in the number of derivative classification decisions. Two agencies reporting substantial percentage decreases in FY 1985, were FEMA (-57%) and Justice (-13%).

Given the wide disparity in figures reported by DoD and CIA for FY 1985, ISOO is concerned that the sampling systems currently in use may not result in the most accurate numbers. Both agencies project the totals based on samples taken over a single one week period. It is likely that in one year the week selected may be relatively quiet while, in another, it may be unusually active. To overcome this potential problem, ISOO is recommending that the DoD and CIA develop systems that sample classification activity during more than a single one week period.

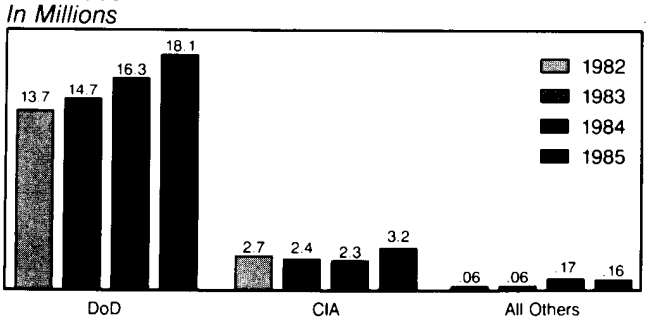
Combined Classification Activity Increases (Exhibit 10)

During FY 1985, the combined number of original and derivative classification decisions was 22,322,895. This was an increase of 2,715,159 (14%) over FY 1984. The primary reasons for the rise were the substantial increases reported by DoD in both original and derivative actions and the 42% increase registered by the CIA in derivative decisions. As in the past, ISOO worked with the agencies whose original or derivative classification decisions accounted for the significant increases to help determine the causes. Among the reasons, several agencies cited greater counterintelligence efforts, particularly in the area of combating international terrorism. As discussed in the section on derivative classification, p. 12, ISOO suspects that the difference is partly the result of sampling that concentrates on one week of the year. In FY 1986, ISOO will devote additional energy to the review of documents during its on-site surveys to ascertain the appropriateness of classification. ISOO will also be seeking greater involvement by the agencies themselves to undertake similar spot checks to determine the propriety of classification decisions.

The percentage of all decisions classified at the "Top Secret" level remained at 2% for the second straight year. However, there was a shift of one percent from "Confidential" to "Secret." The former now comprise 67% of the total, the latter 31%.

DERIVATIVE CLASSIFICATION DECISIONS BY AGENCY **Exhibit 9**

1982-1985
In Millions



COMPARISON OF COMBINED CLASSIFICATION ACTIVITY **Exhibit 10**

FY	Total Actions	% "TS"	% "S"	% "C"
1981	17,374,102	5%	29%	66%
1982	17,504,611	3%	31%	66%
1983	18,005,151	3%	30%	67%
1984	19,607,736	2%	30%	68%
1985	22,322,895	2%	31%	67%

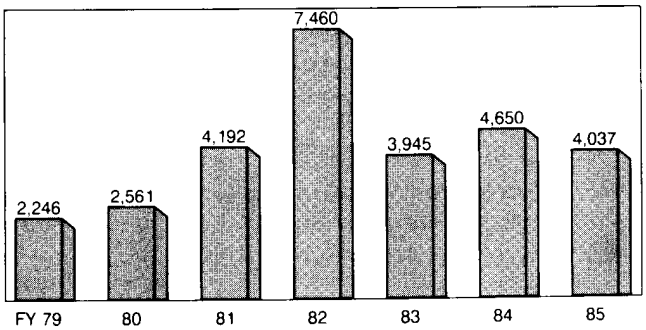
Mandatory Review Continues to Produce Impressive Results (Exhibits 11 through 15)

Under E.O. 12356, the mandatory review process allows agencies or citizens to require an agency to review particular national security information for purposes of seeking its declassification. Such requests must be in writing and must describe the information with enough detail to permit the agency to retrieve it with a reasonable amount of effort. Mandatory review is a process popular with researchers as a less contentious alternative to Freedom of Information Act requests.

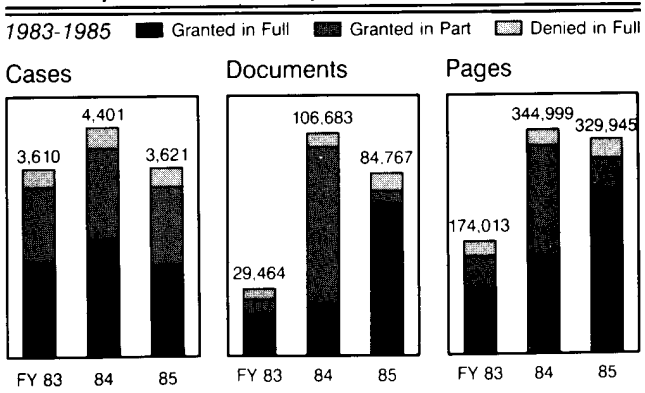
The number of mandatory review requests received in FY 1985, declined by 613 to 4,037. Despite the decrease, this figure represents the fourth highest number of new cases received since the program was instituted in FY 1972. When the 1,523 cases carried forward from FY 1984, are added to the new cases received, agencies had a total caseload of 5,560 during FY 1985. They acted on a total of 3,621 cases, 18% fewer than in FY 1984.

Since FY 1983, ISOO has collected data on agency actions in response to mandatory review requests in terms of cases, documents and pages. A comparison of the figures for each category for the three years indicates that the numbers for FY 1985, are considerably better than those for FY 1983, but not quite as good as those reported in FY 1984. The 3,621 cases acted on in FY 1985, comprised 84,767 documents totaling 329,945 pages. The number of pages acted on was only 4% less than the record number reported for FY 1984.

MANDATORY REVIEW REQUESTS RECEIVED **Exhibit 11**



MANDATORY REVIEW WORKLOAD CASES/DOCUMENTS/PAGES **Exhibit 12**

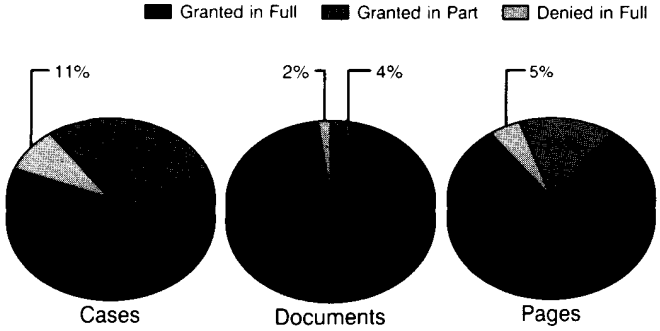


Of the 3,621 cases completed in FY 1985, 1,866 (52%) were granted in full, 1,344 (37%) were granted in part, and 411 (11%) were denied in full. The percentage of cases denied in full marked the first time in three years that the figure exceeded 10%.

Of the 84,767 documents acted on in FY 1985, 79,693 (94%) were granted in full, 3,180 (4%) were granted in part, and 1,894 (2%) were denied in full. The number of documents declassified in full increased by an impressive 54,789 (220%) over the FY 1984 figure. Similarly, the number of pages released in full rose 62% from 163,565 in FY 1984, to 265,197 in FY 1985. This was 80% of the pages reviewed during the last fiscal year. Of the remaining pages, 47,920 (15%) were released in part and 16,828 (5%) were denied in full. During FY 1985, 313,117 pages were either declassified in full or in part, slightly below the combined figure of 325,530 for FY 1984. Nevertheless, the percentage of pages released in full rose to 80% in FY 1985, as compared to 47% in FY 1984. Much of the credit for the improvement rests with DoD, which increased the number of pages released in full from 140,505 in FY 1984, to 207,329 in FY 1985.

E.O. 12356 also gives requesters the right to appeal mandatory review denials to officials of the denying agencies, or, with respect to classified presidential materials, to the ISOO Director. During FY 1985, agencies received 282 new appeals in addition to the 782 carried over from the previous year. Of these 1,064 pending cases, the agencies closed 522 in FY 1985. This represented a notable 23% improvement over FY 1984. Justice was the agency primarily responsible for the improved figure.

MANDATORY REVIEW ACTIONS **Exhibit 13**



FY 1985 MANDATORY REVIEW ACTIONS BY AGENCY **Exhibit 14**

Agency	Total Cases Acted On	% Granted in Full	% Granted in Part	% Denied in Full
State	867	43%	44%	13%
DoD	770	62%	28%	10%
NSC	677	39%	57%	4%
Justice	442	88%	4%	8%
NARA	434	41%	39%	20%
CIA	281	28%	48%	24%
All Others	150	75%	21%	4%
Totals	3,621	52%	37%	11%

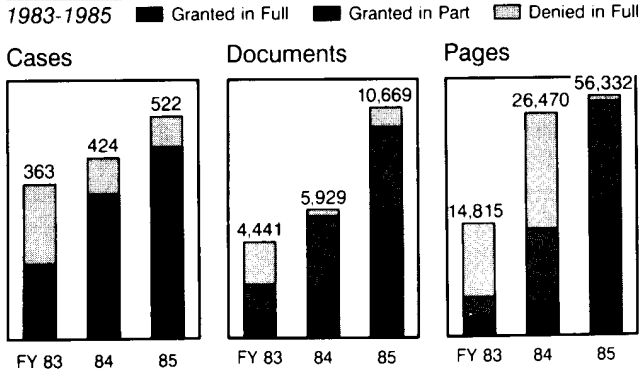
Of the 522 appeals completed, 193 (37%) were granted in full, 262 (50%) were granted in part, and 67 (13%) were denied in full. These appeals totaled 10,669 documents and 56,332 pages, increases of 80% and 113%, respectively, over the figures reported for FY 1984. Of the documents reviewed on appeal during FY 1985, 5,473 (51%) were released in full, 5,036 (47%) were released in part, and only 160 (2%) were denied in full. Of the 56,332 pages reviewed, 28,938 (51%) were declassified in full, 26,750 (47%) were declassified in part, and 644 (2%) remained fully classified. During FY 1985, the numbers of documents and pages released in full or in part showed substantial gains over the comparable figures for the previous year. Documents rose from 5,723 in FY 1984, to 10,509 in FY 1985, while pages released in full or in part increased from 24,791 to 55,688. Once again it was Justice that accounted for the significant improvement in the figures.

Systematic Review Results Disappointing (Exhibits 16 through 18)

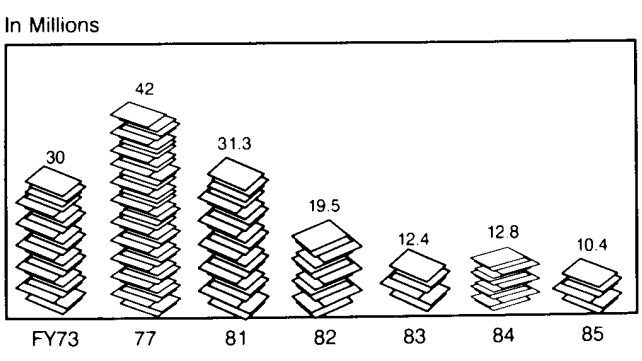
"Systematic review for declassification" is the program, first introduced in 1972, in which classified, permanently valuable (archival) records are reviewed for purposes of declassification after the records reach a specific age. Under E.O. 12356, NARA is required to conduct a systematic review of its classified holdings as they become 30 years old, except for certain intelligence or cryptologic file series which are to be reviewed as they become 50 years old. While other agencies are not required to conduct a systematic review program, they are encouraged to do so if resources are available.

In recent years, the product of the systematic review program has declined as a result of two factors. First, the records that are now being reviewed are not generally susceptible to the bulk declassification methods that were frequently adequate in declassifying World War II era records. Second, the resources available for systematic review have continued to dwindle. From FY 1980 to FY 1983, with the World War II era records almost entirely declassified, the number of pages reviewed under systematic declassification declined precipitously to 12.4 million. Following a call for increased attention by the Assistant to the President for National Security Affairs, in FY 1984, the number increased to 12.8 million pages.

APPEALS WORKLOAD CASES/DOCUMENTS/PAGES **Exhibit 15**



PAGES REVIEWED FOR DECLASSIFICATION **Exhibit 16**

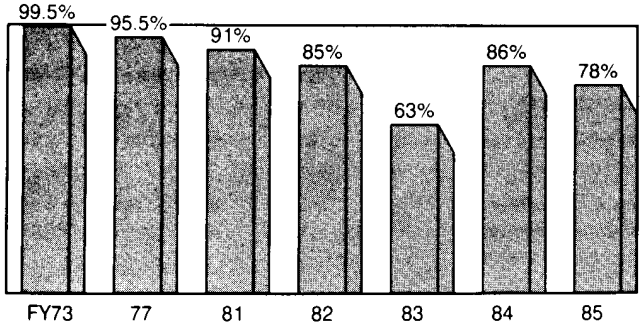


Last year's Report expressed the hope that the slight increase registered in FY 1984, was a sign that the program was on the mend. However, the numbers reported for FY 1985, were the lowest since the program was initiated. During the year, agencies reviewed 10.4 million pages, down approximately 2.4 million (18%) from FY 1984. Of the pages reviewed, 78% were declassified. Although this is lower than the 86% declassification rate reported last year, it is still substantially higher than the 63% registered in FY 1983.

While NARA reviewed 9% more pages in FY 1985 than in FY 1984, this increase was offset by the 29% decline reported by DoD. In FY 1985, DoD reviewed 2.8 million fewer pages under the systematic program than in the previous year. Despite this decline, it is important to note that DoD still reviewed more than 6.8 million pages and declassified just over 5 million pages. Under the Executive order, DoD is not required to conduct any systematic review program. Its voluntary efforts in this area continue to deserve special recognition, and ISOO is hopeful that, at a minimum, DoD will be able to maintain the current program.

Ultimately, the success of the systematic declassification review program rests with NARA. It is the only agency that is required to conduct such a program. A small amount of progress has been made to implement the recommendations of a special task force established by the Archivist of the United States in 1984. There has been some increase in the resources devoted to NARA's systematic review program. Most of NARA's systematic review activity during FY 1985, resulted from a contract between NARA and State to review State's central files through 1955. NARA has signed a similar agreement with AID and has tentatively reached a new agreement with State to review certain of its records through 1959. In spite of these efforts, the 3,141,949 pages reported for FY 1985, is well below the 5 million pages recommended by the Archivist's task force and the 10 million pages that ISOO believes NARA must review annually to ensure a viable systematic declassification program.

PERCENTAGE OF REVIEWED PAGES DECLASSIFIED **Exhibit 17**



FY 1985 SYSTEMATIC REVIEW ACTIONS BY AGENCY **Exhibit 18**

Agency	Pages Reviewed	Pages Declassified	% Declassified
DoD	6,803,568	5,074,439	75%
NARA	3,141,949	2,808,035	89%
AID	352,576	166,062	47%
State	59,345	50,670	85%
Justice	20,767	3,243	16%
DoT	20,000	500	3%
All Others	43,810	4,128	9%
Totals	10,442,015	8,107,047	78%

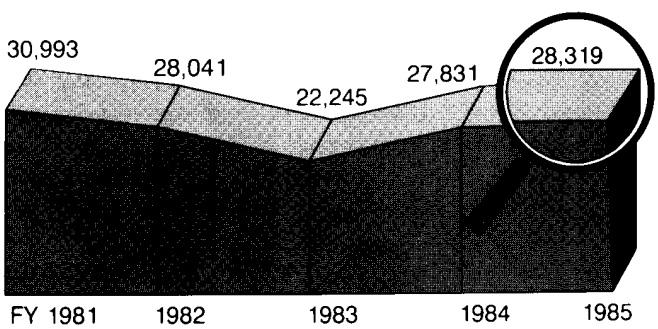
Agency Self-Inspections Increase Marginally (Exhibits 19 and 20)

While the Executive order authorizes the Director of ISOO to conduct on-site inspections of those agencies that generate or handle classified information, it places primary responsibility for internal oversight on the agency heads themselves. The Order requires that agency heads establish and maintain "an active oversight and security education program." Agencies report to ISOO the number of self-inspections that they undertake each year. They also report the number and type of infractions found during the year. Infractions are minor violations of the Order, the implementing ISOO Directive or agency regulations. These statistics do not include the more serious security violations that agencies must report to ISOO as they occur.

For FY 1985, agencies reported that they had conducted 28,319 self-inspections. This was a disappointing 2% increase over FY 1984. Those agencies showing significant decreases included CIA (-14%), DoT (-35%), State (-65%), and Treasury (-53%). Agencies reporting major increases were DoD (+2%), NSC (+93%), and NASA (+46%).

ISOO is concerned not only with the quantity of self-inspections the agencies undertook in FY 1985, but also with their quality. This concern arises from the fact that during the self-inspections conducted in FY 1985, agencies found 4,003 fewer infractions than in FY 1984. The total of 15,154 reported for this fiscal year is 21% lower than the figure for the previous year. The average number of infractions discovered per inspection fell 22% from FY 1984, to FY 1985, to .54. This is far fewer than the number found during ISOO's regular program reviews, and calls into question the thoroughness of the self-inspections the agencies are conducting. ISOO is particularly concerned that agencies increase their review of classified holdings to ascertain the appropriateness of classification and the correctness of security markings.

AGENCY SELF-INSPECTIONS **Exhibit 19**



INFRACTIONS **Exhibit 20**

Infraction	Total FY 82	Total FY 83	Total FY 84	Total FY 85	% Change 84-85
Unauthorized Access	475	620	483	440	- 9%
Mismarking	11,499	10,849	7,503	6,642	- 12%
Unauthorized Transmission	1,197	1,294	1,773	1,688	- 5%
Improper Storage	4,222	3,844	7,363	5,089	- 31%
Unauthorized Reproduction	207	249	190	143	- 25%
Overclassification	290	220	302	164	- 46%
Underclassification	365	317	351	265	- 25%
Classification w/o Authority	392	238	597	109	- 82%
Improper Destruction	665	581	475	322	- 32%
Other	967	132	120	292	+ 143%
Totals	20,279	18,344	19,157	15,154	- 21%

Improving the Information Security System

When the Information Security Oversight Office (ISOO) issued its last Annual Report in April 1985, it was, fittingly, recapping the recent past in order to anticipate the future. Little did ISOO realize, however, how quickly several of its pronouncements would occupy some of 1985's most spectacular news stories. Less than a month later, the FBI's arrest of John Walker commenced the so-called "Year of the Spy," and highlighted the subject of national security information like never before.

In its Report, ISOO expressed ongoing concern about several program weaknesses: The excess of security clearances; the apparent erosion in the "need-to-know" principle; the overdistribution of classified information among and within agencies and offices; and the continuing problem of overclassification, that is, the classification of information whose sensitivity doesn't merit this extraordinary protection. Within weeks of the issuance of the ISOO Report, daily news accounts of the Walker investigation exposed these subjects to the public in a way that ISOO and the rest of the security apparatus within Government could never accomplish.

To be sure, many news accounts grossly exaggerated the link between instances of espionage and perceived weaknesses in the personnel and information security systems. For example, it became almost commonplace for commentators to blame the espionage, in part at least, on the vast numbers of individuals holding security clearances and on the classification of too much information. In each new case, however, the facts belied the logic of these assertions. While far too many people hold unneeded security clearances, all of the accused who held clearances occupied positions that clearly required them. And while the problem of overclassification persists, it is farfetched to establish a direct link between overclassification and espionage. The information at issue in the recent spy cases obviously warranted classification. The actual or intended procurers of the information certainly placed great value upon it, and the Government, in hearing after hearing, has justified the classification of the information to the satisfaction of the judges and juries.

An Opportunity

To the Government's security apparatus, however, the Walker case and its cousins presented something far more important than a challenge -- they presented an opportunity. Upon the release of its FY 1984 Report to the President, ISOO noted little interest within the executive branch to embark upon a program to improve an information security system that ISOO itself pronounced in generally good shape. It was the publicity over the Walker affair that created a hospitable environment in which to attack the problems that continued to nag the system.

ISOO welcomed the opportunity. In July 1985, the National Security Council endorsed ISOO's request to commence an interagency review of the information security system, focusing on five program areas that both the NSC and ISOO perceived as most in need of attention. These were overclassification, or unnecessary classification; the overdistribution of classified information; classification management; revitalization of the "need-to-know" principle; and unauthorized disclosures. That same month the ISOO Director chaired a meeting of representatives of those agencies most heavily involved in the security classification program, including the Departments of State, Treasury, Justice, Defense, Army, Navy, Air Force and Energy, the Central Intelligence Agency, the National Security Agency and the Federal Bureau of Investigation. That meeting produced five task forces, each consisting of at least one civilian and one defense agency, responsible for recommending initiatives pertinent to one of the five problem areas. By the end of October, the interagency group had reached a consensus on thirteen separate initiatives that the ISOO Director transmitted to the Assistant to the President for National Security Affairs.

During testimony before the Senate Select Committee on Intelligence (SSCI) in November 1985, the ISOO Director invited the Committee's

input on the proposed initiatives. Subsequently, the NSC concurred in ISOO's recommendation to invite the input of other interested committees of Congress as well. To date, the NSC and ISOO have received four congressional responses, including a comprehensive package from the SSCI. Each of these responses has endorsed the initiatives wholeheartedly. As this is being written, ISOO is anticipating the NSC's imminent approval to begin those actions necessary to implement the initiatives.

The Initiatives

The thirteen initiatives will not alter the basic structure of the current information security system. Each of the agencies participating in their formulation agreed that the structure of the system established by President Reagan in 1982, is fundamentally sound and, for the most part, working quite well. Rather, the initiatives strive for increased knowledge and increased accountability among the many people who are entrusted with making the system work as it should. Although they are few in number and quite modest in potential cost, ISOO firmly believes that they will spark the improvement of the information security system.

I. Overclassification

The placement of overclassification as the first problem area was intentional. Although the problem of overclassification is not nearly as severe as the popular media portrays it to be, it is a continuing nuisance that eats away at the credibility of the entire system. Critics proclaim that overclassification is the mechanism the bureaucracy uses to hide its mistakes, to shield it from embarrassment, and to cover up its misdeeds. In ISOO's experience, the principal causes of overclassification are far less intriguing. Very few classification decisions are the tools of a cover-up, albeit even one casts a lingering shadow.

Instead, ISOO believes that just about every instance of initial overclassification results from one or more of the following reasons. First, overcaution. Many classifiers believe, and with some reason, that it is better to err on the side of protection than on the side of disclosure. Second, rote classification. It is almost always easier to do things the way they've been done before. Independent thought takes time and effort. Third, status or prestige classification. Some misguided individuals believe that it elevates their stature to elevate the protection of their product. For status classifiers, "Confidential" is never high enough, and "Secret" is merely tolerable. Fourth, and related to status classification, exclusionary classification. This occurs when an official decides that the classification of his product will establish a more exclusive environment, free from routine oversight. Fifth, incorrect, inadequate or nonexistent classification guidance. Poor guidance results in inaccurate derivative classification actions and, quantitatively, is probably the most significant cause of overclassification. And sixth, the lack of portion markings in documents used as sources for derivative classification. If the entire text of a document is classified, even though some portions need not be, documents derived from those portions will be needlessly classified.

There are primarily three initiatives that will attack the problem of overclassification, although others will certainly impact upon it. First, ISOO will issue a directive that establishes minimum requirements for mandatory training of original and derivative classifiers, including those who either issue or use classification guides. Too often these officials are receiving little or no training about the classification system and process, and because of their positions, the agency employees who are supposed to provide this training are reluctant to require it. By mandating training, this directive will provide those responsible with the ammunition they need to enforce adequate familiarity with the information security system. The directive will also require that agencies keep records of the training that each of these officials receives.

Second, ISOO will issue a directive on agency self-inspections that establishes minimum

criteria for internal oversight. This directive will include the requirement that agencies periodically and routinely examine a sample of their classified product to ensure the validity of classification and the existence of appropriate markings. Most current agency self-inspections concentrate almost exclusively on physical security arrangements and largely ignore the information being protected.

Third, ISOO will ask the President to amend Executive Order 12356, "National Security Information," to require employees to report instances of improper classification. Currently, the system strongly encourages, but does not require employees to report classification actions that they believe to be incorrect. In practice, this rarely occurs. If amended, the Order will also require agencies to establish effective procedures for employees to challenge improper classification free from the fear of retribution. This fear is believed to be a primary reason that employees and contractors are not challenging classification decisions today. To be sure, this initiative may result in many unfounded complaints. This seems to be a reasonable price to pay for improving the quality of classification decisions.

II. Overdistribution

The overdistribution of classified information has become a very serious problem in recent years. The widespread availability of copiers and the proliferation of automated information processing systems has multiplied the wholesale distribution of classified information. Increased distribution results in increased security costs and increased vulnerabilities. With much more classified information around, it becomes far more difficult to enforce the requirement that no one, even with a security clearance, may have access to classified information without a job related need to see it. To attack the problem of overdistribution, therefore, is also to help restore the "need-to-know" principle.

Three initiatives confront the problem of overdistribution. First, ISOO will ask the President to issue a statement to the heads of agencies that addresses, among other problem areas, the overdistribution of classified information. A presidential statement will highlight overdistribution as a serious threat to security, not just an administrative burden.

Second, ISOO will amend its current Government-wide directive to require agencies to review, at least annually, the automatic or routine distribution of all classified information. Distributors will be required to update automatic distribution lists and to verify the continuing "need-to-know" of recipients. This initiative should remedy the too frequent situation in which a onetime bona fide recipient is placed on an automatic distribution list and continues to receive the unneeded classified product of the distributor.

Third, ISOO will also amend its current directive to encourage originators of classified information to widen controls on its reproduction, unless there are countervailing reasons to permit uncontrolled reproduction. Currently, "Top Secret" information may not be reproduced without the permission of the originator. Although originators may place similar controls on the reproduction of "Secret" and "Confidential" information, they rarely do so. With copiers available in just about every office, copies of classified documents proliferate. This initative should increase both control and accountability, and reduce the overdistribution of national security information.

III. Classification Management

ISOO has termed the third problem area "classification management." Although classification management is not a new term by any means, here it refers broadly to the management of classified information by classifiers, security specialists, and others whose work has a significant impact upon its creation and handling. The initiatives on classification management will clearly impact as well on each of the other problem areas.

First, ISOO will seek the amendment of E.O. 12356 to identify the management of classified information as an area requiring agency head attention. Specifically, this initiative would

require that the responsibilities for managing classified information be included as critical elements in the performance rating systems of civilian and military personnel who are original classifiers, security managers, or who are otherwise significantly involved in managing classified information. Perhaps more than any other, this initiative will confirm that personal accountability is the most effective means of improving the operation of the information security system.

Second, ISOO will ask that the Assistant to the President for National Security Affairs call upon the Director of the Office of Personnel Management to review and revise the security specialist position series, to include proper recognition for the special skills necessary for the management of classified information. In many respects security specialists occupy the lowest rung of the professional ladder. They receive little respect, low salaries, and few opportunities for advancement. All too often the best people leave the security field as quickly as they can. The Government must improve the professional standing of security specialists, so that it can attract and retain competent, motivated people in these critical jobs.

Third, ISOO will ask that the President direct the Secretary of Defense to study the feasibility of expanding the Defense Security Institute to provide basic training for all executive branch security personnel. Security education plays a fundamental role in assuring the effectiveness of the information security program. Today, however, basic security training is not always available to those who need it. The Defense Security Institute offers an existing school with excellent instructors in the necessary security disciplines. The demand for its courses far exceeds its current capacities. To increase the Institute's course offerings and enrollment, the Secretary of Defense should have the option of seeking reimbursement from the agencies whose employees and contractors would benefit from its expansion.

IV. "Need-to-Know"

The criteria for access to classified information have long been the security clearance plus the "need-to-know". With the proliferation of clearances, reliance upon "need-to-know" becomes even more critical. Instead, there is the clear perception of widespread indifference to this principle. The obvious security threat is not the only unfortunate consequence of the relaxed enforcement of the "need-to-know" principle. Another is the increasing use by agencies of special access programs to help protect classified information. These programs have all too often substituted for the absence of enforced "need-to-know".

The initiatives to attack the overdistribution of classified information should also serve to revitalize the "need-to-know" principle. In addition, ISOO seeks two other initiatives. First, ISOO will ask that the President issue a statement to agency heads that stresses the importance of revitalizing the "need-to-know" principle. To avoid duplication, this would be part of the presidential statement proposed to address other problem areas as well.

Second, ISOO will seek the amendment of E.O. 12356 to require agency heads to ensure effective internal oversight of special access programs, including periodic reconfirmation of their continued need. Special access programs may be established by some agency heads for particularly sensitive information upon a determination that normal management and safeguarding procedures do not control access sufficiently. At present, too many special access programs actually receive less security oversight than normal programs. In addition, a number of these programs are probably unnecessary. This initiative aims for both improved security and increased scrutiny of these costly programs.

V. Unauthorized Disclosures

Unauthorized disclosures is a subject that the executive branch has explored repeatedly in recent years. There are many ongoing and pending actions to deal with this very serious problem. To complement these actions are two additional initiatives. First, ISOO will coordinate with the Security Committee of the Intelligence Community in seeking the development of

educational materials, both unclassified and classified, that address the damage caused by unauthorized disclosures. ISOO is particularly interested in the development of effective, unclassified materials, although it recognizes that the production of these is far more difficult without the aid of classified examples.

Second, ISOO will ask that the President call upon the Attorney General to review and revise existing guidelines on the investigation of unauthorized disclosures. Revised guidelines would cover both internal agency investigations and external investigations by the Department of Justice and the FBI. Currently, investigations of unauthorized disclosures rarely lead to successful prosecutions or even administrative sanctions. Revised investigative guidelines may improve upon this record.

Conclusion: The Unceasing Need for Improvement

Some months ago the Director of ISOO hosted a meeting with an official of an allied democracy. That official had requested the meeting in order to learn more about the American information security system. In describing his government's slow but methodical pace toward greater freedom of information, he cited the American system of access as an ideal, even if flawed, to which all democracies should strive.

That conversation illustrated, perhaps as well as any, the constant irony of the American information security system. Even as other democracies are attempting to cope with the rudiments of open government, officials of the United States Government are struggling to improve the system that protects only a very small portion of the tremendous amount of information it produces every day, so that less, not more information, will remain hidden.

From ISOO's experience, just about every person entrusted with protecting that information wouldn't want it any other way.

Appendix A — DoD Sampling Systems

For most of the agencies that ISOO monitors, the statistics reported each year are based on an actual count of items in each category. From the beginning of ISOO's data collection efforts, however, it was known that such an item-by-item tabulation of classification actions by the agencies with the largest programs was not possible. This was particularly true in the case of DoD, with its large number of components and the enormous volume of its classification activity. Therefore, ISOO agreed that DoD could devise a system to sample the number of its classification decisions, and then project the total for a given fiscal year. ISOO's approval for use of a sampling system, however, did not include the other categories that agencies must report annually, and DoD's data on classification authorities, declassification actions, self-inspections and infractions are based on actual counts.

The original sampling system developed by DoD, and in use since ISOO began collecting program activity statistics, was based entirely on electronically transmitted message traffic. At the time, it was believed to be the only feasible means for DoD to sample its classification activity. Initially, the sample was derived exclusively from the Defense Communications Agency Switch Network Automatic Profile System. Subsequently, NSA also began sampling its message traffic because of its significant involvement in the classification process. Although ISOO approved the message traffic system, ISOO and DoD were never completely satisfied that it was producing the most accurate statistics, because it was believed that message traffic skewed certain statistics about classification, including the raw numbers. Nevertheless, ISOO recognized that the consistent application of this system successfully identified the trends in DoD's classification activity.

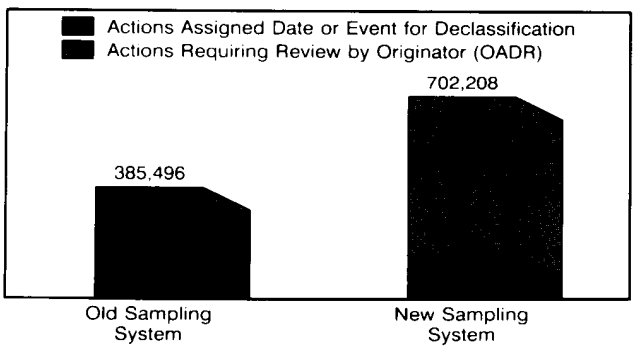
Recently, ISOO and DoD agreed to develop a revised sampling system that would produce more reliable data. As a result, in FY 1985, DoD devised a new method. It requires all DoD components to sample classification actions over a one week period. The numbers obtained are then multiplied by 52. While the figures reported under the revised system are not based entirely on an item-by-item tabulation of original and derivative classification actions, ISOO is convinced that the results are more accurate than those registered under the previous system. First, the sample is not grounded exclusively on message traffic data. The new system includes other document types, including memoranda and reports. Second, the statistics provided are based on data supplied from a greater number of DoD components, including all of the major activities of the military departments, the DIA and NSA.

For FY 1985, DoD used both systems, and reported the results separately. Although ISOO intends to use the data compiled under the new sampling system in future Reports to the President, it did not do so with this Report without first explaining the reasons why the revised method is likely to produce more reliable numbers. For this reason, the main body of the Report reflects the statistics provided by the electronic message traffic system. Use of the revised method at this time would not allow for an accurate analysis of the trends because there are no prior data available for comparative purposes.

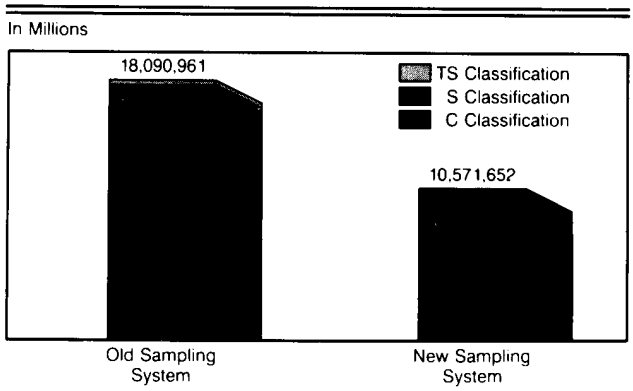
A comparison of the data furnished by the two systems indicates that there are substantial differences. First, the volume of original classification using the new method is considerably higher. Under the previous system, DoD reported 385,496 original decisions. Under the new, the figure is 702,208. Of these, 22% of the original actions were assigned a date or event for declassificaton, as compared to a 71% rate under the old method. By classification level, the number of "Top Secret" original decisions was 9,327 higher under the new system, while "Secret" and "Confidential" actions were 283,547 and 23,838 greater, respectively.

A second difference is that the amount of derivative classification activity is markedly less under the revised sampling system. DoD reported 18,090,961 derivative decisions using the message traffic system, and 10,571,652 utilizing the new method, 42% fewer. There are also significant differences regarding the classification level percentages, except with respect to "Top Secret" actions, which represent 2% of the total under both systems. Using the revised method, "Secret" actions account for 38% of the total, while "Confidential" decisions comprise 60%. Under the old system, the figures were 21% and 77%, respectively.

DoD ORIGINAL CLASSIFICATION **Exhibit A**



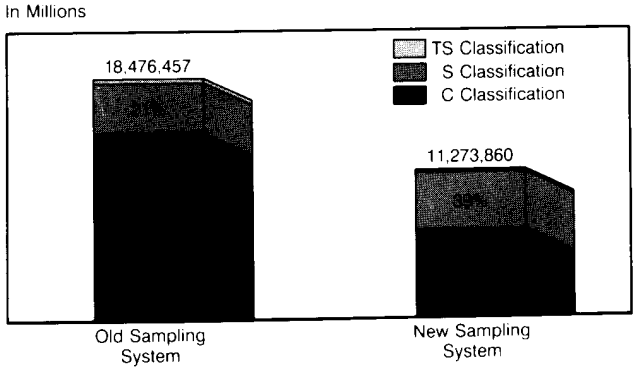
DoD DERIVATIVE CLASSIFICATION **Exhibit B**



Due to significantly fewer derivative decisions, and despite a greater number of original actions, the combined classification reported under the new sampling system is 7,202,597 less than under the old method. Overall classification level percentages also vary considerably, indicating a tendency to classify a greater amount of information at the "Secret" level. Under the new system, 39% of the combined actions are "Secret," while 59% are "Confidential." This is in contrast to the 21%/77% ratio when the old method is utilized.

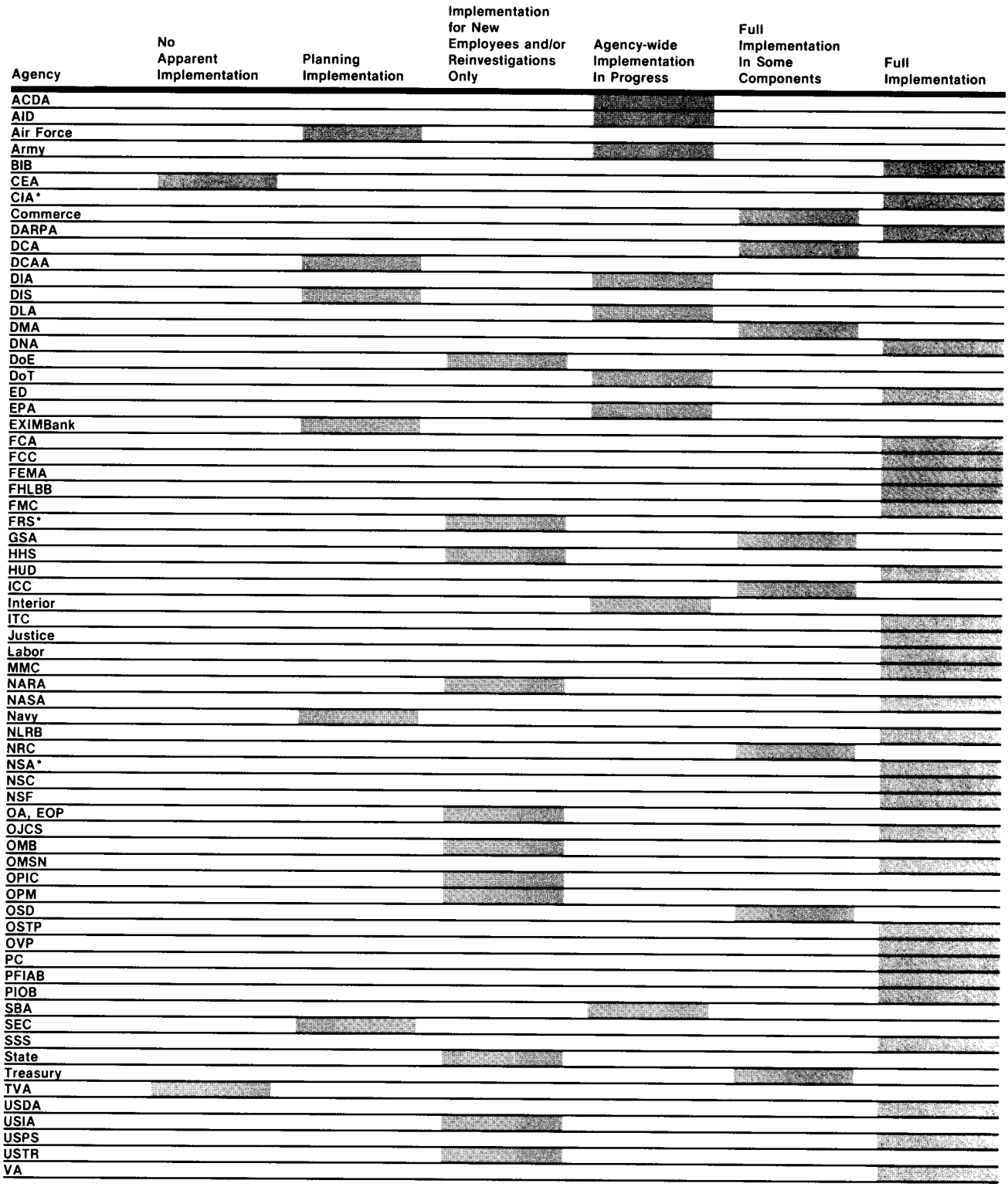
Although ISOO believes that DoD's new system will provide more accurate statistics, it also believes that the system should be refined further. Current instructions require that DoD components undertake the sampling over a single one week period. ISOO is concerned that relying exclusively on such a limited time period may result in skewed numbers. For example, during one year the week selected might be unusually slow in terms of the volume of classified information generated. Thus, the numbers reported will be too low. On the other hand, the week selected the following year might be crisis-ridden and result in unrealistically high figures. To avoid this possibility, ISOO has recommended to DoD and CIA that each agency conduct the sampling of its classification activity on more than one occasion during the year, and then report an average of the data.

DoD COMBINED CLASSIFICATION **Exhibit C**



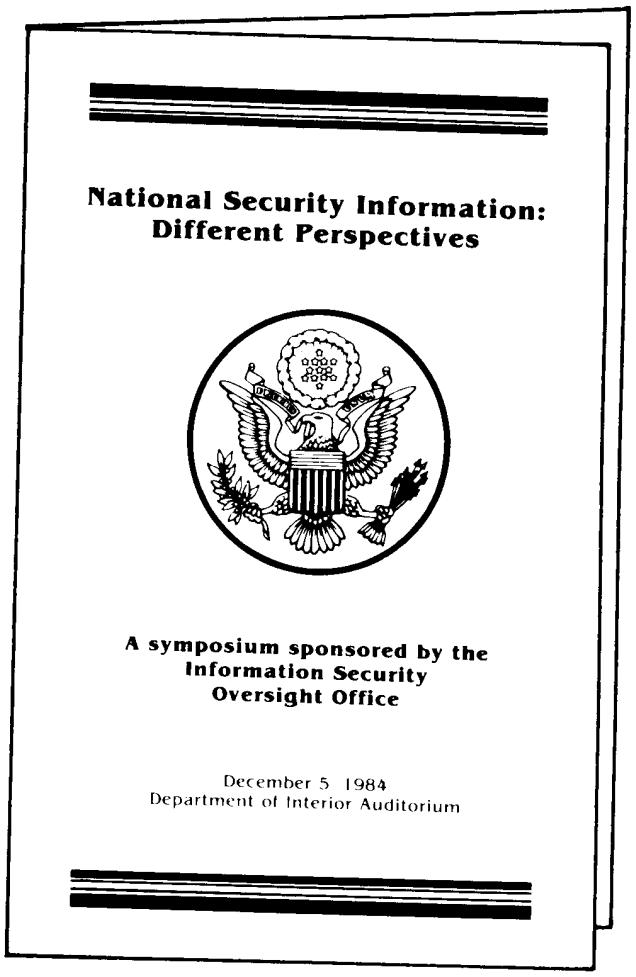
Appendix B - Classified Information Nondisclosure Agreement

Paragraph 1(a) of National Security Decision Directive 84, "Safeguarding National Security Information," of March 11, 1983, directed ISOO to issue a standardized nondisclosure agreement to be executed as a condition of access to classified information. In September 1983, ISOO issued the Standard Form 189, "Classified Information Nondisclosure Agreement," and directed agencies to work toward complete implementation as quickly as possible. The chart below provides an agency by agency breakdown of progress to date.



* Received waiver from NSC to use a substitute form that fully complies with NSDD 84

Appendix C



An audience of 750 from Government, the media and industry heard six noted authorities address their own particular ideas about classified information. The speakers included:

R. Scott Armstrong - Author and former reporter for *The Washington Post*. Current Executive Director, National Security Archive.

Samuel Gammon - Former Ambassador and current Executive Director of the American Historical Association.

Guenter Lewy - Author and Professor of Political Science at the University of Massachusetts.

Mark H. Lynch - Litigator with the American Civil Liberties Union, National Security Project.

Edward F. Sayle - Former Curator of the Central Intelligence Agency's Historical Collection and current editor of *Periscope* Magazine.

Richard K. Willard - Assistant Attorney General, Civil Division, Department of Justice.

The following quotes reflect some of the divergent opinions expressed by the speakers. They are intended as highlights, not comprehensive statements. Arrangements can be made with ISOO for copies of the complete transcript or videotape, or selected excerpts of either.

Scott Armstrong on the source of leaks
The vast majority of the information that makes its way to the newspaper... comes from multiple sources, from multiple interviews, from career bureaucrats. It comes from those people who themselves would not initiate a story or a leak but who will, when faced with a significant disclosure coming out of the room just down the hall from the Oval Office, will correct the information, will put it into context, will say, "That's really not quite right. It really happened this way."

Guenter Lewy on rationalizing unauthorized disclosures
What honestly may appear to the military as information that should be withheld for reasons of security may as honestly appear to the media as information that the American people have a right to know.... The fact that both the media and military act honestly is entirely irrelevant. The question is, "Who should have [the] final say... ?"

Samuel Gammon on declassification
Historians are not just working on the decline and fall of the Roman Empire or the administration of George Washington.... The woods are full of scholars who are toiling away on the Nixon and Ford administration[s] and there are plenty of them already working on Carter, and I daresay some getting started on the [Reagan] administration. So, actually, we want it yesterday, as far as declassification is concerned.

Richard Willard on overclassification
Overclassification can be just as much a danger to an effective information security program as can inadequate classification or inadequate protection.

Mark Lynch on secrecy and public debate
[T]he Manhattan Project and the decision to drop the bomb on Hiroshima... [were] so closely held that the options of not dropping the bomb or dropping a demonstration bomb were never seriously considered.

Scott Armstrong on the law
I can say as a matter of practice that I don't steal and I don't accept stolen property....
The act of dubious legality [is] showing me the information.

Guenter Lewy on journalistic ethics
[T]here's no justification for the view that a citizen who... comes into possession of [a] secret and who knows that it is a secret, should be free to... harm the nation by passing on the secret as he pleases. Journalists too are citizens. They should have the same obligations as anyone else.

Mark Lynch on the scope of Freedom of Information costs
I'm willing to wager that the propaganda public relations efforts of the Department of Defense alone are far greater than the amount of money spent on Freedom of Information processing. The Singing Sergeants, the airplanes that do loop-de-loops at parades and that sort of thing, I'm sure represent a far greater expenditure of funds than FOIA requests.

Edward Sayle on secrecy in American history
Benjamin Franklin and Robert Morris...
looked at the intelligence and they reached an agreement which they committed to paper: "We agree... that it is our indispensable duty to keep it a secret even from Congress. We find by fatal experience the Congress consists of too many members to keep secrets." And they only had 13 colonies.

Richard Willard on preventing a double standard
We need to make it clear that rules on information security apply throughout the administration from the very top to the very bottom. We need to make it clear that people are going to be held to a high level of trust regardless of their position in the administration.

Edward Sayle on the effect of leaks
[U]nless steps are taken to stop this escalating pattern of leaks and to move against those Government employees who are responsible, be it either appointees or careerists, I fear that [a] filtration process may eventually settle in at all levels of this Government, denying our nation's leaders the details essential... for policy level decision making....

Mark Lynch on the perils of compartmentation
[I]f... compartmentation is increased, you may cut down on leaks, but you're also likely to get an increase of ill-conceived operations being put into effect because enough... disinterested people within the policy making arms of the Government won't have an opportunity to render a second, third or fourth opinion.

Samuel Gammon on "intelligence sources and methods"
It is widely rumored, though as far as I know never confirmed, that in 1961, the CIA ran a urinalysis on Khrushchev in Vienna during the summit meeting. A brilliant piece of intelligence work. Possibly what one might call an unauthorized leak.

Edward Sayle on secrecy in American history
When... Tom Paine was determined to have made an unauthorized disclosure of very sensitive diplomatic information, he was dismissed from his job as Secretary to the Foreign Affairs Committee, and stigmatized publicly by a resolution of the Congress. Now that's handling a security violation. ... Do you think we have the same will today?

Scott Armstrong on the source of leaks
The President doesn't have to look very far from his keester to find most of the sources of serious disclosure in this administration.

Richard Willard on misguided disclosures
[T]here are a lot of people in the administration who don't know the difference between an authorized and an unauthorized disclosure. There are probably a lot of political appointees who may think that they're helping out the President, and they really aren't because this President does not believe that every political appointee has the authority to declassify information whenever he thinks it will help with the bureaucratic game.

Samuel Gammon on recovering disclosed information
To the best of my knowledge, even the State Department medics, good as they are, are not competent to perform prefrontal lobotomies on people [who] have learned things. So once its gone, it's gone....

Guenter Lewy on anti-leak legislation
The harm which irresponsible press conduct can do in revealing national security information in some cases will indeed be irreparable.... I do not think it is realistic to rely exclusively on the good will of reporters and editors.... I favor legislation that will give national security information the same protection now available to next year's soybean crop estimate.

Appendix D
ISOO Inspections
FY 1983 - 1985

Agency for International Development
Bureau for Latin America and the Caribbean,
Office of Caribbean Affairs
Bureau for Africa,
Office of East Africa Affairs
Bureau for Asia
Office of Security
Office of the Special Assistant to the
Deputy Administrator

Arms Control and Disarmament Agency
Office of Administration
Communications Section
General Advisory Commission on Arms Control
Bureau of Multilateral Affairs
Bureau of Strategic Programs
Strategic Affairs Division
Bureau of Nuclear Weapons and Control,
International Nuclear Affairs Division

Board for International Broadcasting

Central Intelligence Agency
Directorate of Intelligence
Directorate of Administration
Directorate of Science and Technology
Directorate of Operations
Other Major Activities

Civil Aeronautics Board

Council of Economic Advisers

Defense Advanced Research Projects Agency
Strategic Technology Office
Tactical Technology Office
Defense Science Office
Directed Energy Office
Information Processing Techniques Office
Administrative Services Office

Defense Communications Agency
Headquarters
Joint Data Systems Support Center, Pentagon
Command and Control Systems Organization,
Arlington Hall Station
Defense Communications Engineering Center,
Reston, VA
Joint Data Systems Support Center, Reston, VA

Defense Contract Audit Agency
Security Branch

Defense Industry
American Telephone and Telegraph
Technologies, Inc., Burlington, NC
American Telephone and Telegraph
Technologies, Inc., McLeansville, NC
ITT Electro-Optical Products Division,
Roanoke, VA
Reynolds Metals Company, Richmond, VA
Science Applications International
Corporation, Huntsville, AL
Research Triangle Institute, Research
Triangle Park, NC
CAS Incorporated, Huntsville, AL
Teledyne Brown Engineering, Huntsville, AL
SCI Systems, Inc., Huntsville, AL
BDM International, Inc., Huntsville, AL

Defense Intelligence Agency
Directorate of Security and Counterintelligence
Defense Intelligence College
Directorate for Estimates
Directorate for Scientific and Technical
Intelligence
Directorate for Intelligence and External Affairs
Directorate for Communications
Directorate for Foreign Intelligence
Directorate for JCS Support
Directorate for Research
Directorate of Technical Services and Support

Defense Investigative Service
Headquarters
Capital Region, Alexandria, VA

Defense Logistics Agency
Headquarters
Defense Technical Information Center
Defense Fuel Supply Center

Defense Mapping Agency
Headquarters, Office of Security
Office of Distribution Services
Hydrographic/Topographic Center
Special Security Office

Defense Nuclear Agency
Intelligence and Security Directorate
- Counterintelligence Detachment
- Classification Management Division
- Security and Operations Division

Radiation Directorate
Shock Physics Directorate
Office of the Inspector General
Office of the Deputy Director for Science and Technology
Nuclear Assessment Directorate
Technical Information Directorate

Department of Agriculture
Employee Management and Training Staff (Security)
Foreign Agriculture Service
- Office of Management Services
- Trade Policy, Planning and Analysis Division
- Western Europe and Inter-American Division
- Asia, Africa and Eastern Europe Division
- Communications and Records Cables Division
- Office of Emergency Planning

Department of the Air Force
Assistant Chief of Staff, Intelligence
Assistant Chief of Staff, Information Systems
Deputy Chief of Staff, Plans and Operations
Deputy Chief of Staff, Research, Development and Acquisition
Deputy Chief of Staff, Programs and Resources
1947 Headquarters Support Group - Air Staff
Air Force Systems Command, Andrews AFB
- Electronics Systems Division, Hanscom AFB
- Aeronautical Systems Division, Wright-Patterson AFB
- Foreign Technology Division, Wright-Patterson AFB

Air Force Logistic Command Headquarters, Wright-Patterson AFB
Space Command, Denver, CO
North American Aerospace Defense Command, Denver, CO
Office of Special Investigations, Bolling AFB
Air Force Intelligence Service
Air Force Academy
Strategic Air Command, Offutt AFB

Department of the Army
Assistant Chief of Staff for Intelligence
Deputy Chief of Staff for Operations
Military District of Washington
Criminal Investigation Command
Comptroller of the Army
Logistical Command
Military Traffic Management Command
Office of The Adjutant General
National Guard Bureau
Intelligence and Security Command
Corps of Engineers
Materiel Development and Readiness Command
Missile Intelligence Agency, Huntsville, AL
Ballistic Missile Defense Systems Command, Huntsville, AL
U.S. Army Missile Command, Huntsville, AL
Communications - Electronics Command, Ft. Monmouth, NJ
U.S. Army Natick Research and Development Command, Natick, MA
Army Materials and Mechanics Research Center, Watertown, MA
White Sands Missile Range, Las Cruces, NM
Inspector General
Army Electronics Research and Development Command
Judge Advocate General
U.S. Army Information Systems Command, Ft. Huachuca, AZ
U.S. Army Intelligence Center and School, Ft. Huachuca, AZ

Department of Commerce
Headquarters' Office of Security
National Telecommunications and Information Administration
International Trade Administration
Bureau of the Census
National Oceanic and Atmospheric Administration
Patent and Trademark Office

Department of Education
Office of the Secretary
Office of the Under Secretary
Office of Inspector General
Office of Postsecondary Education
Office of Vocational and Adult Education
Office of Planning, Budget, and Evaluation

Department of Energy
Energy Information Administration
Office of Classification
Office of Computer Services and Telecommunications Management
Office of General Counsel
Office of International Security Affairs
Office of Management and Administration
Office of Safeguards and Security

Department of Health and Human Services
Office of the Assistant Secretary for Health
Office of the Secretary
Food and Drug Administration
National Institutes of Health

Department of Housing and Urban Development
Immediate Office of the Secretary
Assistant for International Affairs
Assistant Secretary for Administration
Inspector General

Department of the Interior
Headquarters' Office of Security
U.S. Geological Survey
Bureau of Mines
Office of the Secretary
Office of the Solicitor
Office of Environmental Project Review
Office of the Assistant Secretary - Water and Science
Office of Information Resources Management
Assistant Secretary - Land and Minerals Management

Department of Justice
Federal Bureau of Investigation
Immigration and Naturalization Service
Drug Enforcement Administration
- El Paso Intelligence Center

Bureau of Prisons
Foreign Claims Settlement Commission
Main Justice
- Antitrust Division
- Civil Division
- Criminal Division
- Justice Management Division
- Tax Division
- Office of Intelligence Policy and Review
- Office of Information and Privacy

Department of Labor
Office of Emergency Preparedness Planning (Information Security)
Bureau of International Labor Affairs
Bureau of Labor Management Relations and Corporate Programs

Department of the Navy
Office of the Chief of Naval Operations
Naval War College, Newport, RI
Naval Underwater Systems Center, Newport, RI
Naval Underwater Systems Center, New London, CN
Naval Intelligence Support Center
Naval Research Laboratory
Joint Cruise Missile Project Office
Office of Command Control
U.S. Atlantic Fleet Headquarters, Norfolk, VA
Commander Naval Surface Forces, U.S. Atlantic Fleet, Norfolk, VA
Headquarters Fleet Marine Force Atlantic, Norfolk, VA
Commander Submarine Force, U.S. Atlantic Fleet, Norfolk, VA
Commander Naval Surface Forces Pacific, San Diego, CA
Space Command and Control Directorate
Navy Ocean Systems Command, San Diego, CA
Marine Corps Base, Camp Pendleton, CA

Department of State
Classification/Declassification Center
Information Systems Office
Information Systems Security Staff
Office of Security
- Domestic Operations
- Education and Training Staff

Bureau of Intelligence and Research
- Office of the Executive Director
- Office of Economic Analysis
- Office of Analysis for Inter-American Republics

Bureau of East Asian and Pacific Affairs: Japan
United States Mission to the United Nations, New York, NY
- Office of Administrative Affairs
- Reference Section
- Political Section
- Economic and Social Section
- Communications Section
- Security
- Resources Management

Bureau of European Affairs
- Office of Soviet Union Affairs

Bureau of Inter-American Affairs
- Office of Central American Affairs
- Office of Caribbean Affairs

Bureau of Politico - Military Affairs
- Office of Strategic Nuclear Policy

U.S. Embassy, Ottawa, Canada
- Office of the Deputy Chief of Mission
- Personnel Section
- Political Section
- Economic Section
- Administrative Counsellor

Department of Transportation
Office of the Secretary
Federal Aviation Administration
United States Coast Guard: Headquarters; Miami; New Orleans;
El Paso Intelligence Center, El Paso, TX;
National Narcotics Border Interdiction System, Miami, FL
Maritime Administration
Federal Highway Administration

Department of the Treasury
Office of the Secretary
U.S. Customs Service
Internal Revenue Service
U.S. Secret Service
Bureau of Alcohol, Tobacco, and Firearms
Bureau of Engraving and Printing
Bureau of Public Debt
Bureau of Government Financial Operations
Comptroller of the Currency
Bureau of the Mint

Environmental Protection Agency
Facilities and Support Services Branch
Personnel Security Division
Office of the Associate Administrator for International Activities

Executive Office of the President, Office of Administration

Export-Import Bank

Farm Credit Administration

Federal Communications Commission
Office of Science and Technology
Office of Plans and Policy
Mass Media Bureau
Emergency Communications Division
Internal Review and Security Division

Federal Emergency Management Agency
Emergency Operations Directorate
Office of Security
Document Control Branch
National Preparedness Programs Directorate

Federal Home Loan Bank Board

Federal Maritime Commission
Bureau of Investigations
Office of Policy Planning and International Affairs

Federal Reserve System
Office of Security
International Information Center

General Services Administration
Office of Internal Security
Federal Property Resources Service
Information Resources Management Service

International Trade Commission

Interstate Commerce Commission
Office of Compliance and Consumer Assistance
Staffing and Employee Relations, Personnel Office

Marine Mammal Commission

National Aeronautics and Space Administration
Office of Aeronautics and Space Technology
Office of Space Science and Applications
Office of Space Flight
Office of Space Tracking and Data Systems
Goddard Space Flight Center
John F. Kennedy Space Center, Kennedy Space Center, FL

National Archives and Records Administration
Administrative Services Division
Records Declassification Division
Lyndon B. Johnson Library, Austin, TX
Nixon Presidential Materials Project

National Labor Relations Board

National Science Foundation

National Security Agency

National Security Council

National Transportation Safety Board

Nuclear Regulatory Commission
Office of International Programs
Office of the Deputy Executive Director for Operations
Standardization and Special Projects Branch
Division of Security
- Information Security Branch
- Facilities Personnel Security Branch
- Systems Security Branch
- Policy and Operational Support Branch

Division of Technical Information and Document Control
- Records Services Branch

Office of Nuclear Material Safety and Safeguards
Division of Rules and Records

Office for Micronesian Status Negotiations

Office of Management and Budget

Office of Personnel Management
Personnel Security Division
Compliance and Investigations Group

Office of Science and Technology Policy

Office of the Secretary of Defense
Executive Secretariat
Under Secretary of Defense for Policy
Assistant Secretary of Defense for International Security Policy
Assistant Secretary of Defense for International Security Affairs
Net Assessment
Defense Guidance Staff
Emergency Planning
Assistant Secretary of Defense for Health Affairs
Assistant Secretary of Defense for Legislative Affairs
General Counsel
Under Secretary of Defense for Research and Engineering
Assistant Secretary of Defense, Comptroller
Assistant Secretary of Defense, Manpower, Installations and Logistics
Assistant Secretary of Defense for Reserve Affairs
Assistant Secretary of Defense for Public Affairs
Inspector General
Defense Security Assistance Agency
Assistant to the Secretary of Defense for Atomic Energy
Washington Headquarters Services
Assistant to the Secretary of Defense (Intelligence Oversight)
Program Analysis and Evaluation

Office of the United States Trade Representative

Office of the Vice President

Organization of the Joint Chiefs of Staff
Office of the Secretary
Office of the Director, Joint Staff
Office of the Chairman
Manpower and Personnel Directorate
Operations Directorate
Logistics Directorate
Plans and Policy Directorate
Support Services Directorate
Joint Analysis Directorate
Command, Control and Communications Systems Directorate
Joint Planning Staff for Space
Strategic Plans and Resource Analysis Agency
Joint Special Operations Agency
United States Readiness Command, Tampa, FL
United States Central Command, Tampa, FL

Overseas Private Investment Corporation

Peace Corps

President's Foreign Intelligence Advisory Board

President's Intelligence Oversight Board

Securities and Exchange Commission

Selective Service System

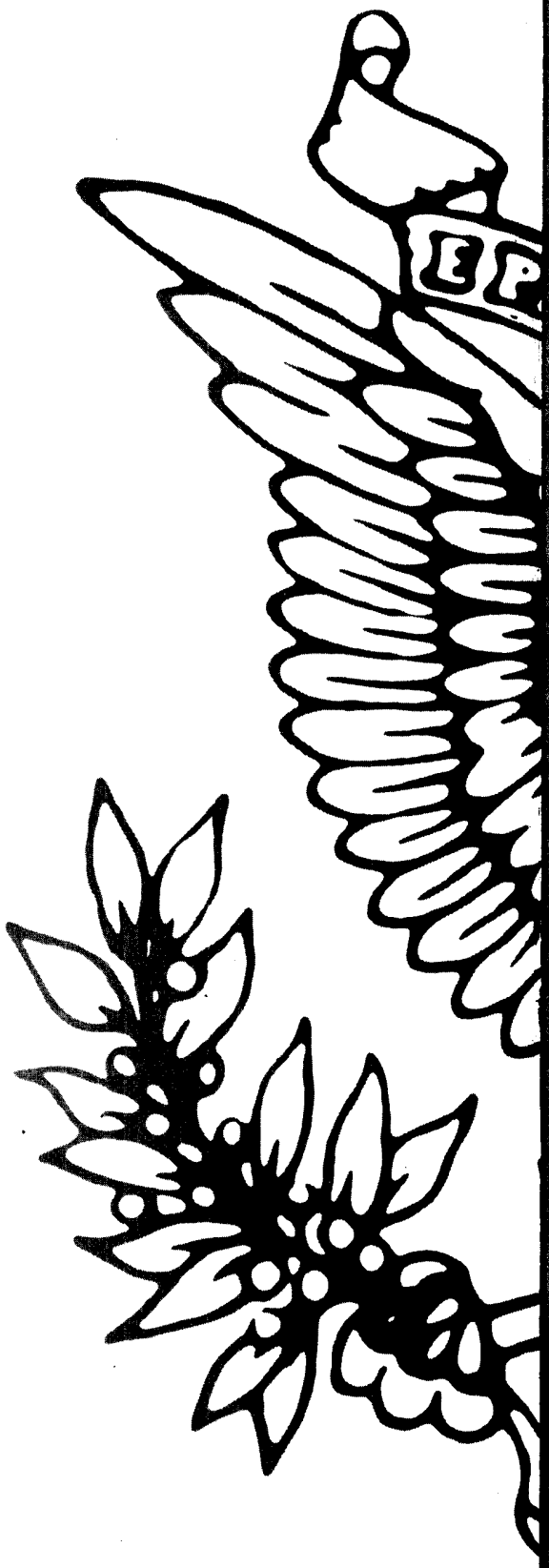
Small Business Administration
Physical and Personnel Security Branch

United States Information Agency
Office of Security
Physical Security Division
Office of American Republics Affairs
Office of North African, Near Eastern, and South Asian Affairs
Office of Public Liaison
Office of Administration and Technology
Classified Library
Bureau of Management
Secretariat Staff
Afghan Media Staff
Office of International Visitors
Office of East Asian and Pacific Affairs
Communications Center

United States Postal Service
Office of the Chief Postal Inspector
Inspection Service

Veterans Administration
Assistant Inspector General for Policy, Planning and Resources
Department of Medicine and Surgery
Office of Data Management

Information Security Oversight Office



Washington, D.C. 20405