


Annual Report
to the President
FY 1984



Information Security
Oversight Office





General
Services
Administration

Information Security
Oversight
Office

Washington, DC 20405

April 26, 1985

The President
The White House
Washington, DC 20500

Dear Mr. President:

I am pleased to submit the Information Security Oversight Office's (ISOO) 1984 Report to the President.

Established under Executive Order 12065 and continued under Executive Order 12356, effective August 1, 1982, the ISOO oversees the information security system throughout the executive branch. The ISOO is an administrative component of the General Services Administration, but receives its policy direction from the National Security Council.

Last year I was able to report that the system you had established under E.O. 12356 had worked remarkably well during its first full year of operation. This year I can state that this initial success has continued. The agencies of the executive branch are providing better protection for national security information, while also working diligently to control and eliminate unwarranted classification and other shortcomings.

Critical to the success of the system has been the support that you and your senior officials throughout the executive branch have contributed. I urge your continued involvement and assistance.

Respectfully,

A handwritten signature in cursive script that reads "Steven Garfinkel".

STEVEN GARFINKEL
Director

Contents

| | Page |
|--|------|
| Letter to the President..... | i |
| Agency Acronyms or Abbreviations..... | iv |
| Summary of FY 1984 Program Activity..... | v |
| The Information Security Program FY 1984..... | 1 |
| Program Reviews and Inspections..... | 2 |
| Statistical Reporting..... | 2 |
| Original Classification Authorities..... | 3 |
| Original Classification..... | 5 |
| Derivative Classification..... | 9 |
| Total Classification Activity..... | 10 |
| Mandatory Review for Declassification..... | 11 |
| Systematic Declassification Review..... | 15 |
| Agency Self-Inspections..... | 18 |
| Narrative Look at FY 1984..... | 20 |
| Appendix: ISOO Inspections: FY 1983 and FY 1984..... | 27 |

Exhibits

| | |
|---|----|
| 1. Reduction in Original Classifiers..... | 4 |
| 2. Number of Original Classifiers..... | 4 |
| 3. Comparison of Original Classification Activity.... | 5 |
| 4. Original Classification Decisions..... | 6 |
| 5. FY 1984 Original Classification Decisions by Agency..... | 7 |
| 6. Original Classification Decisions Scheduled for Automatic Declassification..... | 8 |
| 7. Comparison of Derivative Classification Activity.. | 9 |
| 8. FY 1984 Derivative Classification Actions by Agency..... | 10 |
| 9. Comparison of Combined Classification Activity.... | 10 |
| 10. Original vs. Derivative Classification..... | 11 |
| 11. Mandatory Review Requests Received..... | 12 |
| 12. Mandatory Review Actions..... | 13 |
| 13. FY 1984 Mandatory Review Actions by Agency..... | 14 |
| 14. Mandatory Review Appeals Received..... | 15 |
| 15. Pages Reviewed for Declassification..... | 16 |
| 16. Percentage of Reviewed Pages Declassified..... | 17 |
| 17. FY 1984 Systematic Review Actions by Agency..... | 17 |
| 18. Agency Self-Inspections..... | 18 |
| 19. Infractions..... | 19 |

Agency Acronyms or Abbreviations Used in this Report

| | | |
|----------|---|--|
| ACDA | : | Arms Control and Disarmament Agency |
| AID | : | Agency for International Development |
| CIA | : | Central Intelligence Agency |
| DoD | : | Department of Defense |
| DoE | : | Department of Energy |
| DoT | : | Department of Transportation |
| FBI | : | Federal Bureau of Investigation |
| FEMA | : | Federal Emergency Management Agency |
| GSA | : | General Services Administration |
| ISOO | : | Information Security Oversight Office |
| JUSTICE | : | Department of Justice |
| NARA | : | National Archives and Records Administration |
| NARS | : | National Archives and Records Service |
| NASA | : | National Aeronautics and Space Administration |
| NRC | : | Nuclear Regulatory Commission |
| NSC | : | National Security Council |
| OSTP | : | Office of Science and Technology Policy |
| OVP | : | Office of the Vice President |
| PIOB | : | President's Intelligence Oversight Board |
| STATE | : | Department of State |
| TREASURY | : | Department of the Treasury |
| USIA | : | United States Information Agency |
| USTR | : | Office of the United States Trade Representative |

Summary of FY 1984 Program Activity

The FY 1984 Report to the President is the second 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 declined 2% in FY 84, to 6,900, the first time the figure has fallen below 7,000.
- . Original classification decisions increased slightly in FY 84, to 881,943; this was still considerably less than the 1,055,152 original decisions made in FY 82, under E.O. 12065.
- . By classification level, 2% of original classification decisions were "Top Secret", 30% were "Secret", and 68% were "Confidential".
- . Under E.O. 12356, originally classified information has been marked for automatic declassification 33.5% of the time, as compared to an estimated 10% of the time under E.O. 12065.
- . Derivative classification decisions rose 9% over FY 83, to 18,725,793.
- . 4% of all classification actions were original, 96% were derivative.
- . The total of all classification actions, 19,607,736, represented a 9% increase over FY 83.

Declassification Activities

- . Agencies received 4,650 new mandatory review requests, the second highest total since the program was established in FY 72.
- . Agencies processed 4,401 requests, and declassified the information in whole or in part in 91% of the cases, releasing in whole or in part 104,821 documents totaling 325,530 pages.
- . Agencies received 408 new mandatory review appeals.
- . Agencies took action on 424 appeals, declassifying additional information in whole or in part in 82% of the cases.
- . Under the systematic review program, agencies declassified 10.9 million pages of permanently valuable records, 3 million more than in the previous year.

Inspections

- . Agencies undertook 27,831 self-inspections, a 25% increase over FY 83.
- . Agencies reported 19,157 infractions, a 4.4% increase over FY 83.

Information Security Oversight Office

The Information Security Program

FY 1984

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 highlights Government-wide performance during FY 1984, the system's second 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 1984, ISOO's budget was \$649,000.

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. During FY 1984, this also included the issuance of rules regarding agency use of a Classified Information Nondisclosure Agreement (Standard Form 189) to be executed by each employee as a condition of access to classified information. Second, ISOO conducts on-site inspections or program reviews of monitored agencies on a regular basis. Third, it gathers, analyzes and reports statistical data on agencies' programs. Fourth, it evaluates, develops or disseminates security education materials and programs. 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. 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. The appendix to this Report lists those activities that ISOO inspected during FY 1983 and FY 1984.

These on-site inspections 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 they 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, 1983 through September 30, 1984.

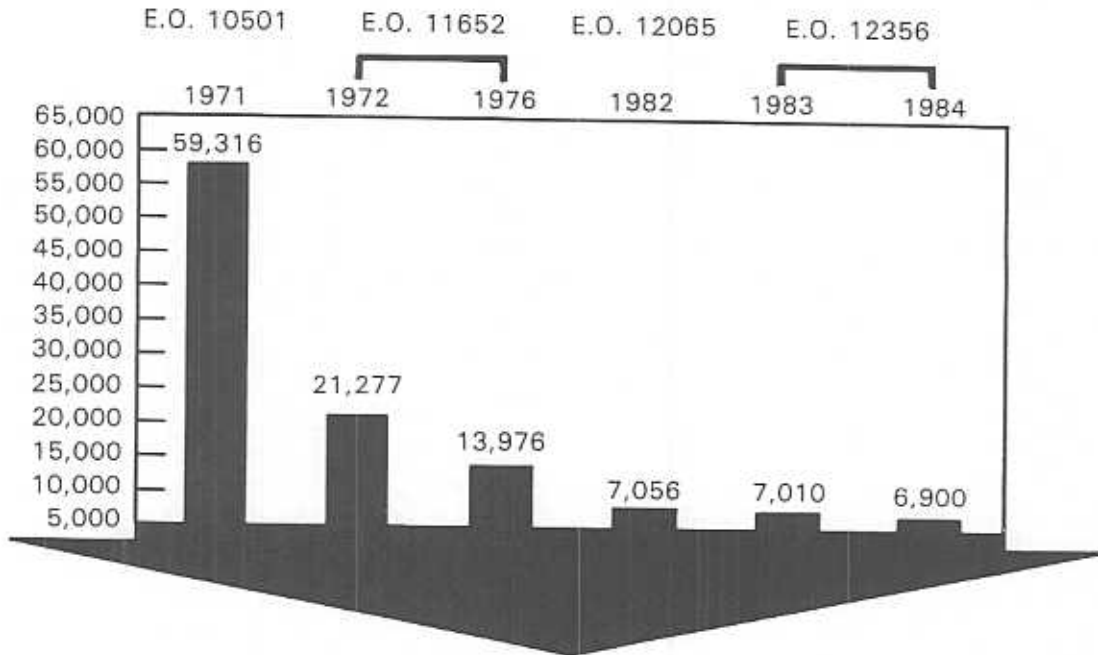
Further Reductions of Original Classification Authorities

(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 prods agencies to conduct regular surveys to ensure that the number of original authorities is in line with operational requirements.

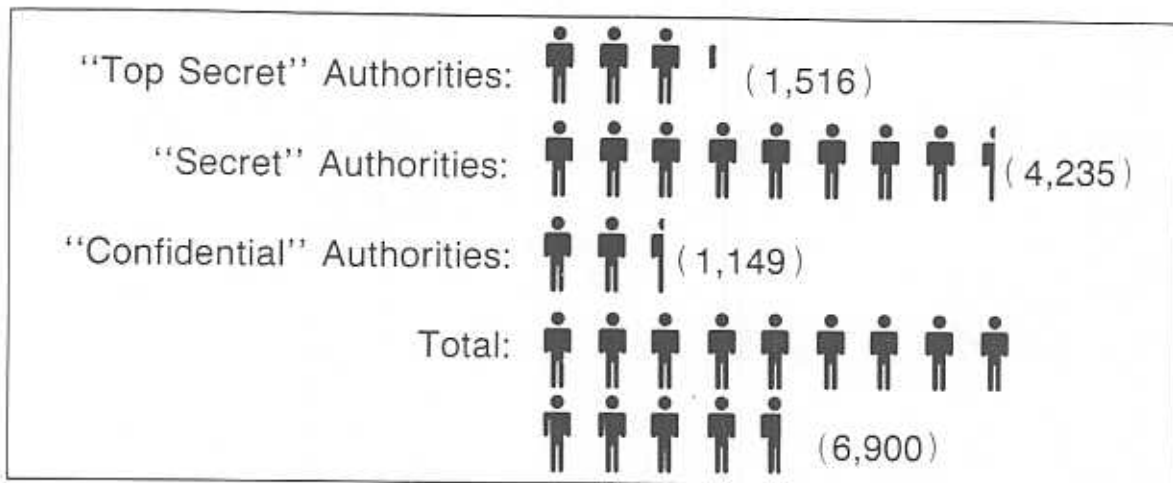
In 1972, there were 59,316 individuals in the executive branch authorized to classify originally. This number has decreased dramatically since that time. In FY 1984, there were only 6,900 original classification authorities. This figure represents a decrease of 2% from the 7,010 original classifiers reported in FY 1983. The overall reduction results from a decline of 180 (14%) in the number of "Confidential" classifiers. This figure more than offsets the rise in the number of "Top Secret" classifiers by 35 (2%), and "Secret" by 35 (1%).

Exhibit 1
The Reduction in Original Classifiers
1971 - 1984



Several agencies deserve special credit for significantly reducing the number of original classifiers in FY 1984. They include ACDA (-31%); DoD (-9%); NRC (-8%); Treasury (-30%); and OVP (-33%). Of particular note is ACDA, which has reduced its number of original classifiers from 88 in FY 1982, to 33 in FY 1984. In FY 1985, ISOO will focus particular attention on those activities which increased their number of original classifiers in the past year.

Exhibit 2
Number of Original Classifiers



 = 500 Authorities

Original Classification Remains at Reduced Level

(Exhibits 3 through 6)

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.

During FY 1984, the number of original classification decisions totaled 881,943. This represents an increase of 17,844 from the number reported in FY 1983. "Top Secret" actions increased by 3,824 (24%), "Confidential" rose by 29,946 (5%), while the number of "Secret" actions dropped by 15,926 (6%). Despite the increases reported for FY 1984, the number of original classification actions were only 2% higher than the prior year's unprecedented low figure. The total remains 16% lower than the 1,055,152 actions reported for FY 1982, the last year under the previous Executive Order.

Exhibit 3
Comparison of Original Classification Activity

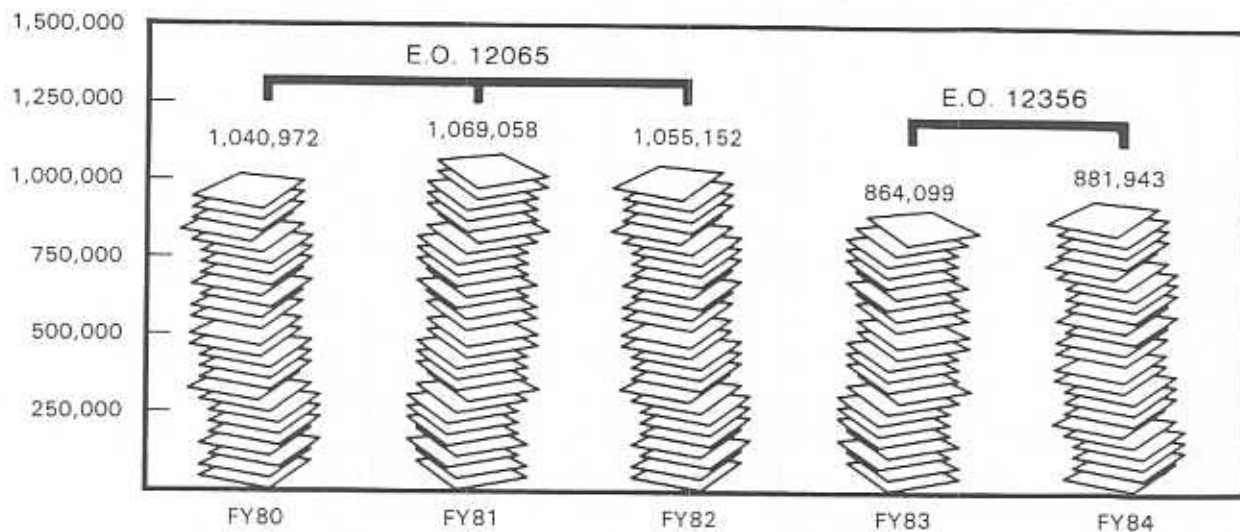
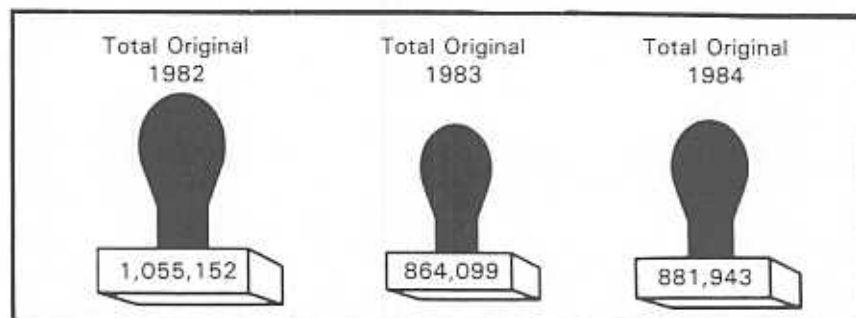
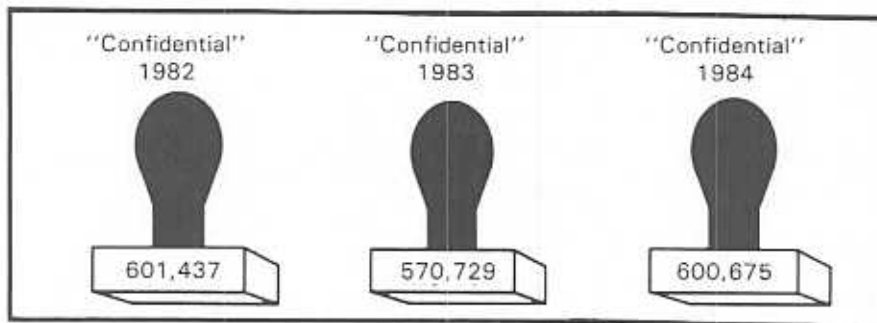
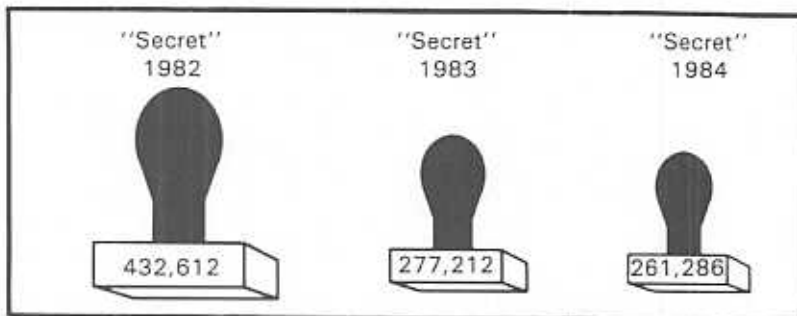
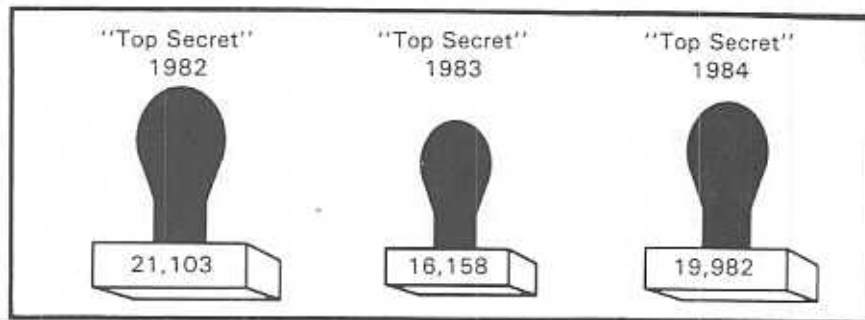


Exhibit 4

Original Classification Decisions



In FY 1984, "Top Secret" decisions comprised 2% of original classification actions, "Secret" accounted for 30%, and "Confidential" the remaining 68%. These figures closely approximate those reported for FY 1983. "Confidential" determinations still constitute a significant majority of original classification actions made in the executive branch. This has important implications in terms of the costs borne by the Government to protect national security information. More stringent requirements in terms of storage and transmission apply to "Secret" and especially "Top Secret" information. Therefore, classifying at the "Confidential" level rather than "Secret" or "Top Secret" saves the Government considerable resources. More importantly, holding the line on classification and classification levels helps preserve the integrity of the classification system itself.

Four agencies continue to classify originally more than 99% of the actions within the executive branch. Of these, CIA registered a 16% increase (following a 44% decrease in FY 1983), DoD a rise of 11%, and State an increase of 8% during FY 1984. These increases were nearly offset by a dramatic decrease of 51% at Justice. In preparation for this Report, ISOO worked with the agencies primarily responsible for the rise in original classification decisions to ascertain the reasons for the increases. ISOO is satisfied that the increases in original classification actions are reasonably accounted for by a number of factors. These included several specific world events that gave rise to large numbers of classified communications as well as new defense and intelligence initiatives.

Exhibit 5

FY 1984 Original Classification Decisions by Agency

| Agency | Original Decisions | % Assigned Date or Event for Declassification | % OADR (Must Be Reviewed before Declassification) | % "TS" | % "S" | % "C" |
|------------|--------------------|---|---|--------|-------|-------|
| DoD | 345,919 | 71% | 29% | 1% | 18% | 81% |
| CIA | 266,188 | 5% | 95% | 5% | 42% | 53% |
| State | 196,052 | 12% | 88% | 0% | 22% | 78% |
| Justice | 64,942 | 0% | 100% | 3% | 63% | 34% |
| Treasury | 2,028 | 16% | 84% | 0% | 7% | 93% |
| FEMA | 1,945 | 5% | 95% | 30% | 44% | 26% |
| DoE | 1,506 | 15% | 85% | 0% | 60% | 40% |
| AID | 1,099 | 68% | 32% | 0% | 1% | 99% |
| All Others | 2,264 | 34% | 66% | 5% | 35% | 60% |

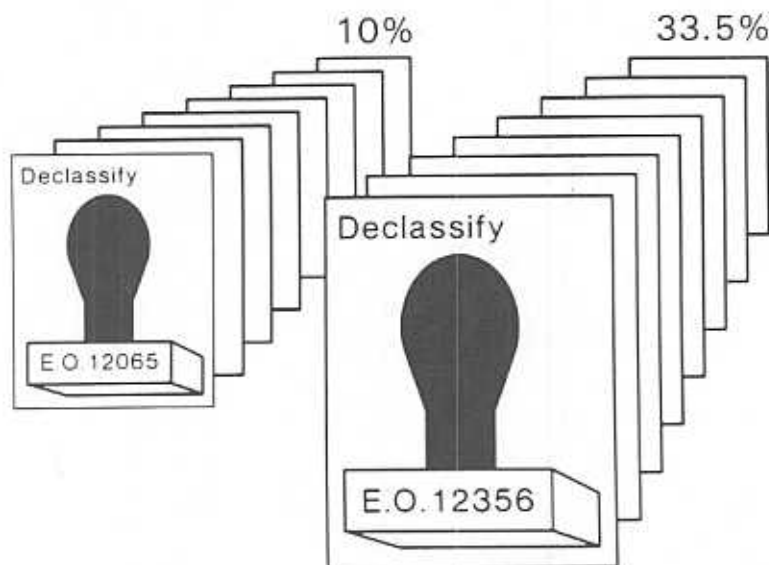
During FY 1984, 32% of the actions specified automatic declassification upon the passage of a particular date or event. Although this figure is slightly less than for FY 1983, the 33.5% average under E.O. 12356 still represents a substantial improvement over the predecessor system, which ISOO estimates required agency review prior to declassification in 90% of original classification actions.

Automatic scheduling for declassification should facilitate the declassification process as a whole and increase the amount of material made available to scholars and the public.

DoD continues to merit special recognition with an automatic declassification rate of 71%, the same proportion as reported in FY 1983. Other agencies had significantly lower ratios. ISOO will continue to encourage these activities to use a specific date or event as the declassification instruction whenever possible, and will examine documents to determine whether such instructions could reasonably substitute for the indefinite designation "Originating Agency's Determination Required" ("OADR").

Exhibit 6

Original Classification Decisions Scheduled for Automatic Declassification



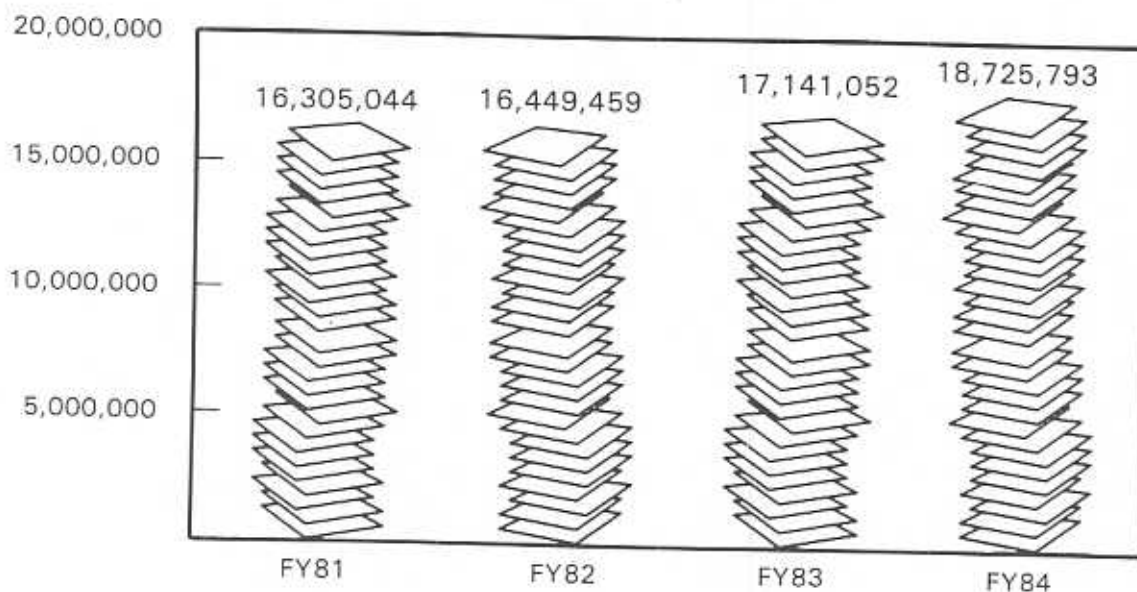
Derivative Classification Actions Increase

(Exhibits 7 and 8)

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.

During FY 1984, executive branch agencies made 18,725,793 derivative classification decisions, a 9% increase over FY 1983. Of the total derivative classification actions taken during the reporting period, 459,385 (2%) were classified at the "Top Secret" level, 5,525,987 (30%) at the "Secret" level, and 12,740,729 (68%) at the "Confidential" level. "Top Secret" derivative decisions decreased from 3% to 2% of the total number of decisions. There were 63,143 fewer "Top Secret" derivative decisions in FY 1984 than in FY 1983, a decrease of 12%.

Exhibit 7
Comparison of Derivative Classification Activity



Of the three agencies responsible for nearly all of the derivative classification actions, DoD and Justice reported increases of 1,602,689 and 99,213 actions respectively. The CIA experienced a decline of 128,827 actions. Other agencies reporting substantial percentage reductions in the number of derivative classification decisions in FY 1984 as compared to FY 1983 included the PIOB (-92%), NSC (-34%), OSTP (-41%), USTR (-62%), and Treasury (-44%).

Exhibit 8
FY 1984 Derivative Classification Actions by Agency

| Agency | Total Derivative Actions | % "TS" | % "S" | % "C" |
|------------|--------------------------|--------|-------|-------|
| DoD | 16,264,038 | 2% | 21% | 77% |
| CIA | 2,289,872 | 3% | 83% | 14% |
| Justice | 124,927 | 1% | 99% | 0% |
| DoE | 18,262 | 0% | 17% | 83% |
| NASA | 11,265 | 0% | 99% | 1% |
| FEMA | 4,453 | 8% | 65% | 27% |
| Treasury | 1,527 | 2% | 62% | 36% |
| All Others | 11,449 | 27% | 29% | 44% |

Combined Classification Activity Increases

(Exhibits 9 and 10)

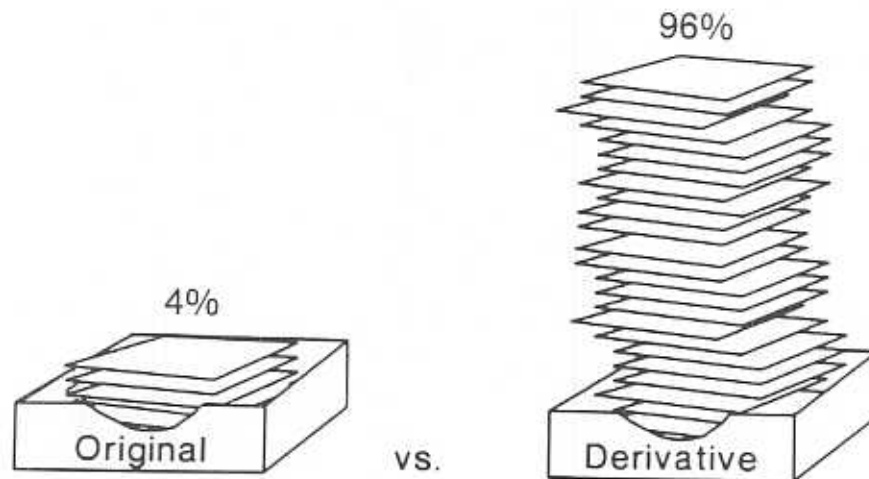
During FY 1984, the combined number of original and derivative classification decisions made by executive branch agencies was 19,607,736. This was approximately 1,600,000 (9%) more than in FY 1983, an increase that is larger than the corresponding increases reported during the past several years. The overriding reason is the 9% rise in derivative actions; original decisions had almost no bearing on the increase.

Exhibit 9
Comparison of Combined Classification Activity

| 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% |

For FY 1984, the data show 2% of all classification decisions were classified at the "Top Secret" level, 30% at the "Secret" level, and 68% at the "Confidential" level. This ratio reflects a 1% decrease in "Top Secret" decisions, and a 1% increase in "Confidential" decisions. As in previous years, DoD (84.7%) and CIA (13%) accounted for almost 98% of the classification activity in the executive branch. During FY 1984, the ratio of original to derivative classification actions changed for the second year in a row. Prior to FY 1983, original classification comprised 6% of all classifications, and derivative 94%. By FY 1984, the ratio was 4% original, 96% derivative. The reason for this change and its impact are examined in the narrative that follows this section of the Report.

Exhibit 10 Original vs. Derivative Classification



Mandatory Review Yields Impressive Results

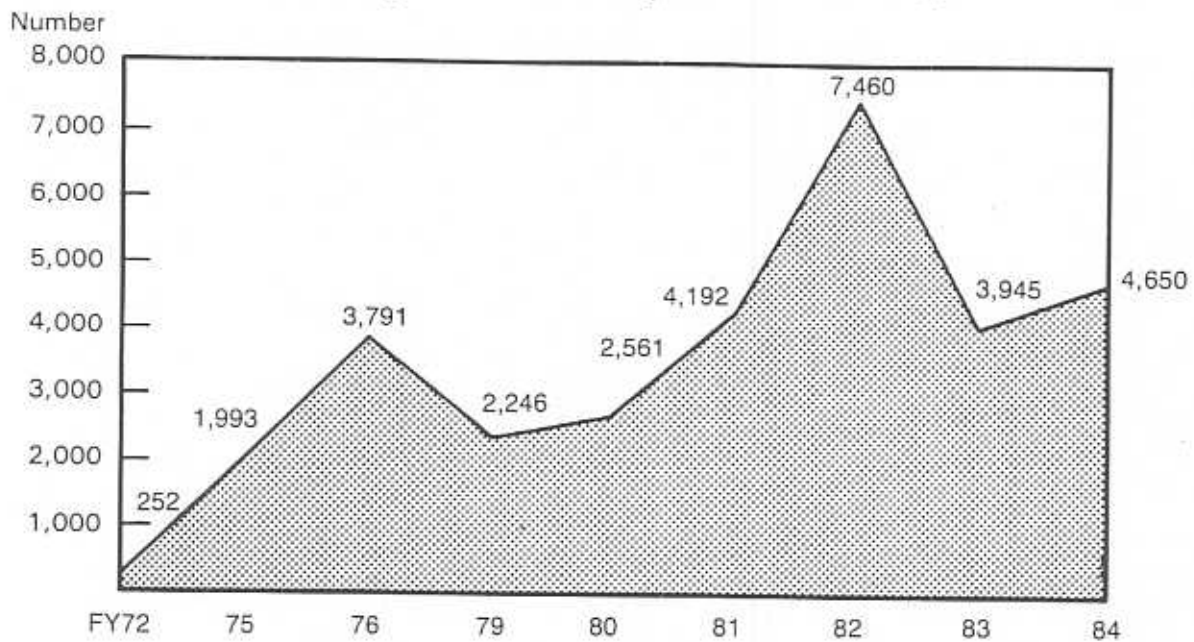
(Exhibits 11 through 14)

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 combative alternative to Freedom of Information Act requests.

After leveling off in FY 1983, the number of mandatory review requests increased again in FY 1984 to 4,650. This is the second highest number of requests received since the program was established in FY 1972. Added to the 1,334 cases carried forward from FY 1983, agencies had a mandatory review caseload of 5,984 during FY 1984. Of these, the agencies processed 74% of the total, a 28% increase over the proportion processed in FY 1983. In last year's report, ISOO indicated that one of its immediate goals would be to seek to reduce the inventory of pending cases. While progress toward this goal was offset by the 18% increase in new cases received, agencies exhibited excellent initiative by acting on 22% more cases, 262% more documents, and 98% more pages than in FY 1983.

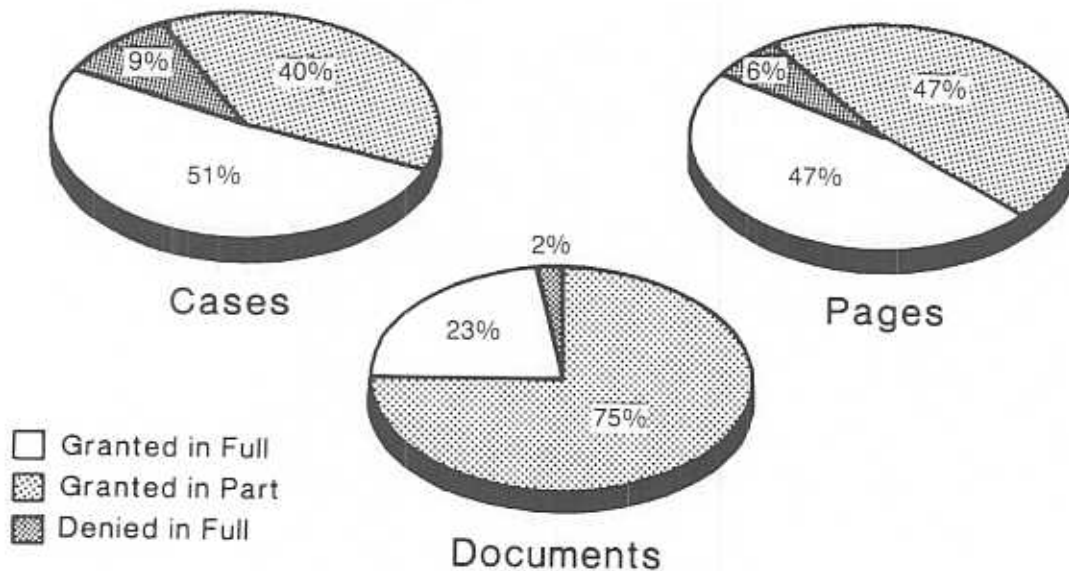
Exhibit 11

Mandatory Review Requests Received



ISOO collects data on agency actions in response to mandatory review requests in terms of cases, documents and pages. Of the 4,401 cases acted on in FY 1984, 2,259 (51%) were granted in full, 1,759 (40%) were granted in part, and 383 (9%) were denied in full. Although the percentage of cases granted in full decreased marginally in FY 1984, the percentage of cases denied in full remained below 10% for the second consecutive year.

Exhibit 12
Mandatory Review Actions



The 4,401 cases comprised 106,683 documents or 344,999 pages of national security information, an increase of 77,219 documents and 170,986 pages over the figures for FY 1983. Of the 106,683 documents, 24,904 (23%) were declassified in full, 79,917 (75%) were declassified in part, and 1,862 (2%) remained fully classified. Although the percentage of documents fully declassified dropped markedly, the percentage of documents which remained fully classified also decreased. A clearer indication that the mandatory review program resulted in a greater amount of information being declassified is reflected in the number of pages released in full or in part during the year. Of the 344,999 pages reviewed in FY 1984, 325,530 were either declassified in full or in part, over twice as many as the 154,238 pages reported for FY 1983.

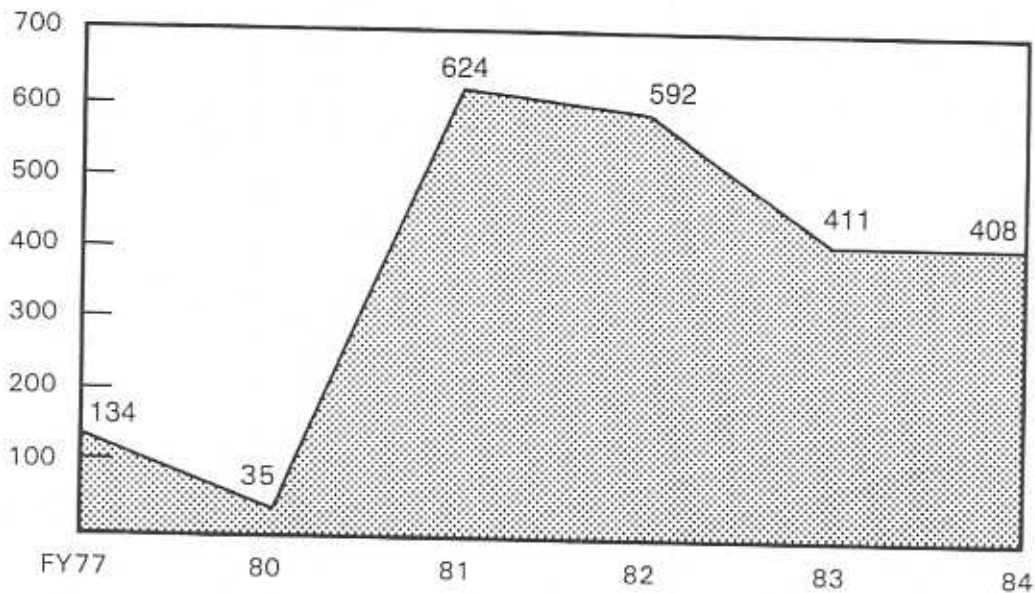
Exhibit 13
FY 1984 Mandatory Review Actions by Agency

| Agency | Total Cases Acted On | % Granted In Full | % Granted In Part | % Denied In Full |
|----------------------|-------------------------|----------------------|----------------------|---------------------|
| DoD | 1,732 | 52% | 42% | 6% |
| State | 684 | 47% | 45% | 8% |
| NSC | 645 | 49% | 44% | 7% |
| GSA (Including NARS) | 422 | 40% | 41% | 19% |
| Justice | 339 | 78% | 19% | 3% |
| CIA | 274 | 33% | 44% | 23% |
| All Others | 305 | 63% | 25% | 12% |

The Executive Order also gives requesters the right to appeal mandatory review denials to designated officials of the denying agencies, or, with regard to classified presidential materials, to the Director of ISOO. During FY 1984, agencies received 408 new appeals in addition to 802 appeals carried over from the previous year. Of these 1,210 pending appeals, the agencies completed 424 (35%) in FY 1984. This was a 4% improvement over FY 1983, but ISOO will continue to urge increased efforts to reduce the remaining backlog.

Of the 424 appeals processed, 92 (22%) were granted in full, 256 (60%) were granted in part, and 76 (18%) were denied in full. These 424 appeals comprised 5,929 documents or 26,470 pages. Of the 5,929 documents reviewed on appeal, 1,997 (34%) were declassified in full, 3,726 (63%) were declassified in part, and 206 (3%) remained fully classified. Of the 26,470 pages reviewed, 6,729 (26%) were declassified in full, 18,062 (68%) were declassified in part, and 1,679 (6%) remained fully classified. For FY 1984, the numbers of documents and pages declassified and released in full or in part were substantially higher than in FY 1983. This suggests that the agencies are making every effort to release as much information as possible consistent with national security concerns.

Exhibit 14
Mandatory Review Appeals Received



Systematic Review May Be On The Mend

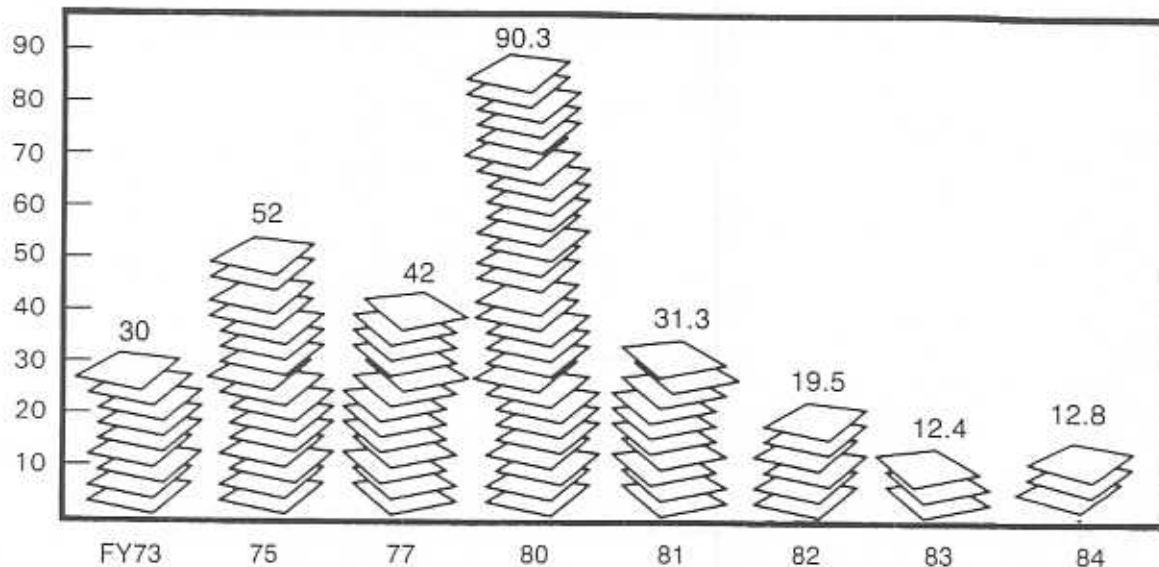
(Exhibits 15 through 17)

"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, NARS (now 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, the number of pages reviewed under the systematic declassification program decreased from 90.3 million to 12.4 million.

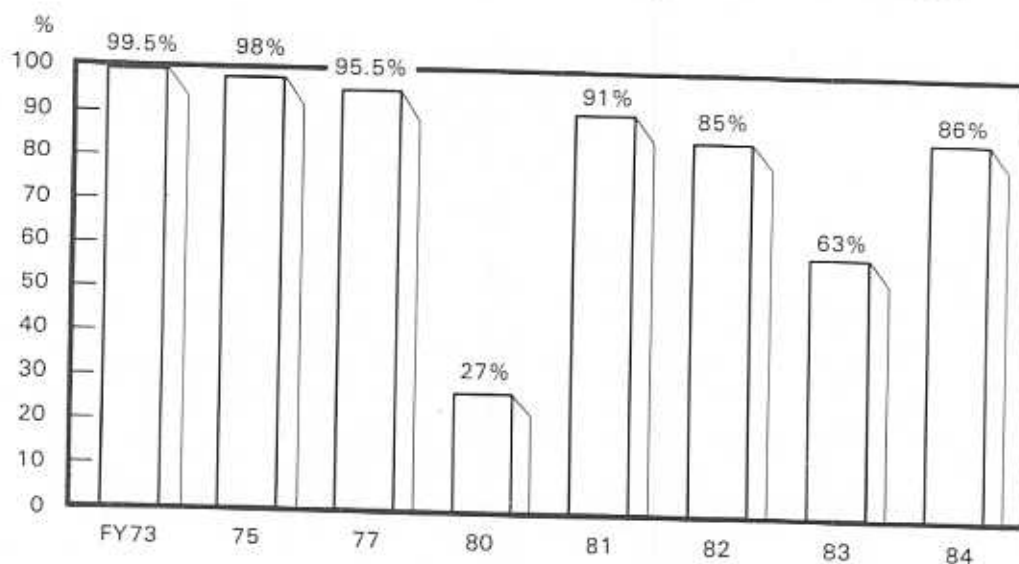
Exhibit 15 Pages Reviewed for Declassification

In Millions



Increased attention to the systematic review program in the past year may signal a reversal of that trend. For FY 1984, agencies reported that they had reviewed nearly 12.8 million pages, an increase of 366,000 pages over FY 1983. Of even greater importance is the substantial increase in the percentage of reviewed pages that were declassified under the program in FY 1984. In FY 1983, only 63% of the pages reviewed were declassified; that figure jumped to approximately 86% for the period covered by this Report. In other words, of the 12.8 million pages reviewed in FY 1984, 10.9 million were declassified. This represents an increase of more than 3 million pages in the amount of historically valuable Government records made available to the public as a result of the program compared to the prior year. These improved figures are primarily the work of DoD, at which the percentage of pages declassified rose from 54% in FY 1983, to 85% in FY 1984. DoD accounts for over 75% of all the pages reviewed under the systematic declassification program. NARA, which is required under E.O. 12356 to conduct a systematic review program, and which accounts for the second highest volume, increased by 1% the number of pages examined, and declassified 91%. It is hoped that the resources made available for the NARA program will be greater in the next fiscal year. A task force established by the Archivist in FY 1984, on which the ISOO Director served, recommended a substantial increase in the size of the NARA staff devoted to the program, and there has been some progress in this direction.

Exhibit 16
Percentage of Reviewed Pages Declassified



Although agencies other than NARA are not required to conduct systematic review programs under E.O. 12356, several continue to do so. In addition to DoD, State and USIA have active programs, although the number of pages reviewed by the latter two agencies dropped 47% and 74%, respectively. In the case of USIA, the decrease resulted from the fact that its resources had to be devoted to a significant increase in its mandatory review workload. On the other hand, DoE's systematic review effort increased substantially in FY 1984, and the proportion of pages declassified by DoE was nearly 100%.

Exhibit 17
FY 1984 Systematic Review Actions by Agency

| Agency | Pages Reviewed | Pages Declassified | % Declassified |
|------------|----------------|--------------------|----------------|
| DoD | 9,628,592 | 8,186,052 | 85% |
| GSA/NARS | 2,889,600 | 2,641,954 | 91% |
| State | 56,517 | 51,330 | 91% |
| USIA | 40,000 | 39,950 | 99% |
| DoT | 25,000 | 2,548 | 10% |
| All Others | 133,881 | 8,944 | 7% |

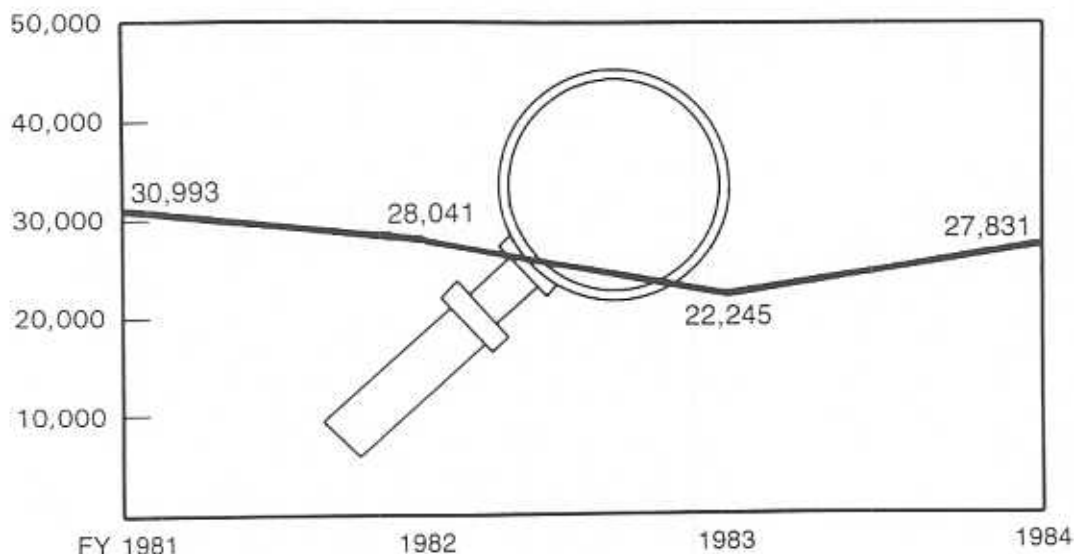
Agency Self-Inspections Increase

(Exhibits 18 and 19)

While the Executive Order authorizes the Director of ISOO to conduct on-site inspections of those agencies that generate and 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.

During FY 1984, the number of agency self-inspections totaled 27,831, a 25% increase over FY 1983. In last year's report, ISOO expressed concern about the decline in the number of agency inspections. As a result, during its own inspections program, ISOO analysts have repeatedly stressed the need for agencies to develop internal monitorship programs to ensure effective implementation of the Order. One of the consequences of the increased number of self-inspections undertaken by the agencies was a corresponding rise in the number of infractions reported.

Exhibit 18
Agency Self-Inspections



The total number of infractions reported for FY 1984 was 19,157, an increase of 4.4% over FY 1983. Although ISOO applauds the 25% rise in self-inspections conducted by the agencies, they continue to detect less than one infraction per inspection, which is far below the average that ISOO analysts find during their on-site surveys.

Exhibit 19
Infractions

| Infraction | Total FY 81 | Total FY 82 | Total FY 83 | Total FY 84 | % Change 83-84 |
|------------------------------|----------------|----------------|----------------|----------------|-------------------|
| Unauthorized Access | 476 | 475 | 620 | 483 | -22% |
| Mismarking | 8,797 | 11,499 | 10,849 | 7,503 | -31% |
| Unauthorized Transmission | 924 | 1,197 | 1,294 | 1,773 | +37% |
| Improper Storage | 3,341 | 4,222 | 3,844 | 7,363 | +92% |
| Unauthorized Reproduction | 135 | 207 | 249 | 190 | -24% |
| Overclassification | N/R | 290 | 220 | 302 | +24% |
| Underclassification | N/R | 365 | 317 | 351 | +11% |
| Classification w/o Authority | N/R | 392 | 238 | 597 | +150% |
| Improper Destruction | N/R | 665 | 581 | 475 | -18% |

N/R = Statistics not reported for FY 1981

A Narrative Look At FY 1984

The President's issuance of Executive Order 12356 prompted unprecedented scrutiny and discussion of the Government-wide information security program. Never before had the classification, declassification, and safeguarding of national security information generated so much attention and comment. Then, with the issuance of the Information Security Oversight Office (ISOO) FY 1983 Report to the President, the commotion abruptly subsided. For many, unfortunately, good news was no news.

ISOO's analysis of FY 1984, the second full year of E.O. 12356's operation, brings more good news. It is now very clear that the outstanding accomplishments of the prior year were no fluke. While a number of hurdles remain, ISOO concludes once again that the President's stated goal of achieving better protection for national security information while working to prevent unwarranted classification is clearly being met.

FY 1984 Program Strengths: General

(a) Following quite naturally upon the smooth transition from E.O. 12065 to E.O. 12356 has been the continued stability of the revised system. Last year ISOO noted two contributing factors to the smooth transition: First, the two systems paralleled one another in most day-to-day situations; and second, the concerted effort of senior program officials throughout the executive branch to achieve a smooth transition. For FY 1984, ISOO cites a third factor as contributing significantly to the continued stability of the system. This is the increased administrative flexibility deliberately built into E.O. 12356.

As noted by ISOO in its FY 1982 Report to the President, one of the predecessor system's glaring shortfalls was its inflexibility in a number of administrative situations. While designed to prevent excessive classification, in practice several of these provisions simply produced excessive red tape. E.O. 12356 modified these provisions to allow controlled flexibility within the system.

From all indications the result is a system that is stable but not static. Within the executive branch concerned officials and employees express widespread satisfaction with the revised system. Outside the executive branch, in particular among those institutions most frequently critical of the information security system, there is quiet, except for an occasional outburst over initiatives to impede unauthorized disclosures of classified information. Perhaps more than anything else this very silence bespeaks the current stability of the information security system.

(b) The absence of serious abuse is critical to the credibility of a system that exists to control access to national security information. In ISOO's view, once again in FY 1984, no serious abuse of the system surfaced. The oversight and responsiveness of senior program officials contributed significantly to its absence.

Of particular concern to ISOO is the potential for abuse of that provision of E.O. 12356 that permits, under very limited circumstances, the reclassification of information that has previously been declassified and disclosed under appropriate authority. Once again in FY 1984, reclassification actions very seldom arose. When they did, ISOO examined their legitimacy in detail. In each instance, ISOO was either satisfied that the reclassification action was necessary and proper or the agency involved withdrew its plans for reclassification.

(c) In its last Report to the President ISOO faulted the lack of familiarity with E.O. 12356 by too many persons who work with classified information. As a result, during FY 1984, ISOO again concentrated much of its oversight on agency security education programs. While there is still significant room for improvement in some agencies, most have instituted training programs that have increased employees' knowledge about the information security system and their responsibilities under it. A greater percentage of persons interviewed by ISOO analysts during its FY 1984 inspections displayed a good working knowledge of information security than had been the case in prior years. With the continuation and augmentation of security education efforts, ISOO anticipates even more improvement in this area.

FY 1984 Program Strengths: Statistical

(a) As ISOO has repeatedly maintained, the most important quantitative measurement of the information security system is the annual tally of original classification decisions. More precisely than any other reported statistic, these decisions represent the number of "new secrets" created during the year. In actual practice, of course, the number of "new secrets" is far lower than the total number of original classification decisions. There is large scale subject matter duplication, and many classification decisions that some agencies count as original are actually derivative.

In FY 1983, the executive branch witnessed a dramatic 18% drop in the number of original classification decisions. FY 1984's minimal 2% increase reveals that this was not a one-shot fluke. Original classification remained well below the levels experienced under E.O. 12065, despite a year that featured a number of world events that generated large numbers of classified communications. In ISOO's view, the major reason for the decrease in original classification relates to the greater use of classification guides, especially in agencies that did not use guides until recently. The discussion below, concerning the rise in derivative classification, examines this phenomenon in greater detail.

(b) The agencies, especially the many components of the Defense establishment, continue to do an excellent job of designating a significant portion of their classified information for automatic declassification upon a specific date or event. The percentage of information so marked under E.O. 12356 remains more than three times greater than under the prior system. Ultimately, that much more information will be available to public access without involving a costly, time-consuming review procedure.

(c) In the wake of a new information security system, which required agency heads to redesignate their original classifiers, FY 1983's reduction of 46 classifiers was a pleasant surprise. The agencies demonstrated responsible restraint at a time when some excess would have been understandable, given the fact that the number of original classifiers had shrunk by more than 50,000 over the prior 12 years.

In FY 1984, the agencies did even better, shaving another 110 classifiers off the rolls. There is some temptation to accept this first dip below the 7,000 range as an achieved goal. Only the knowledge that there are still a number of unnecessary original classification authorities prevents this complacency.

(d) In FY 1982, the number of mandatory review requests took a sudden upswing. Critics explained that researchers had turned to the mandatory review process because the dwindling product of systematic review no longer met their needs. In FY 1983, the number of mandatory review requests leveled off. These same critics explained that researchers had discovered that the mandatory review process wasn't worth the effort. ISOO is hard-pressed to anticipate the "Catch-22" explanation for FY 1984.

In fact, the mandatory review process has been, and continues to be, an outstanding success. Year in and year out, agency reviewers declassify a large percentage of the information sought by researchers. In FY 1984, the mandatory review workload, when expressed by the number of documents and pages examined, increased to what was probably its highest level. (ISOO did not collect data in terms of documents and pages until FY 1983.) As a result, researchers received a higher return than ever before. The agencies, which rarely receive anything for their efforts but more criticism, deserve a great deal of credit.

FY 1984 Program Weaknesses: General

(a) Section 4.1 of Executive Order 12356 expresses the link between the information security and personnel security systems:

A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.

These requirements are routinely paraphrased as "a clearance plus a 'need-to-know.'" In ISOO's view both of these requirements deserve far greater attention.

With respect to the clearance process, commentators for many years have been calling for reform, but the agencies have never been able to agree among themselves what changes are necessary or advisable. In National Security Decision Directive 84, the President instituted a high-level, interagency effort to resolve these problems, and that process is continuing. Whatever the system, however, ISOO believes that far too many individuals receive clearances for access to national security information. Its inspections and its experience with agency implementation of the Classified Information Nondisclosure Agreement constantly reinforce this fact to ISOO. All too often, agencies grant clearances by habit, or as a badge of prestige, rather than as a requisite of job responsibilities. Far greater efforts are needed to limit national security clearances to persons whose work necessitates access to national security information.

Perhaps more damaging is the widespread indifference to the "need-to-know" principle. All too often holders of classified information distribute it to others based solely on their clearances, making little or no effort to ascertain the reasons access is required for the performance of job responsibilities. With the proliferation of clearances, strict adherence to "need-to-know" becomes even more critical.

In ISOO's view, the obvious security threat is not the only unfortunate consequence of relaxed enforcement of personnel security requirements. Another is the increasing usage by agencies of special access programs to help protect classified information. Under E.O. 12356 and its predecessor systems, certain agency heads may create special access programs "to control access, distribution, and protection of particularly sensitive information . . ." These programs are very costly. ISOO believes that many current special access programs would not have been created if agencies had greater confidence in the enforcement of clearance and "need-to-know" principles.

(b) Similar security problems flow from the broad distribution of classified information among and within agencies and offices. Too often, classified information is distributed to others by rote rather than reason. Increasingly, the use of automated systems exacerbates this problem. Programmers frequently design these systems to facilitate the widespread distribution of information rather than its protection. As a result, offices routinely receive the classified product of other offices whether or not they have any need for the information.

A disturbing side effect of the broad distribution of classified information involves its impact on the unauthorized disclosure of national security information. First, widespread availability heightens the opportunity for negligent or deliberate unauthorized disclosure; subsequently, when unauthorized disclosures occur, many investigations of them fail because of the size of the universe of possible leakers.

(c) Even with greatly reduced levels of original classification, overclassification remains a problem and, indeed, a threat to the credibility of the system. From ISOO's broad exposure to national security information, the amount that is classified unnecessarily is far less than critics of the system proclaim. Nevertheless, the "bad apple" syndrome haunts the classification process. Reduced numbers do not permit the relaxation of oversight.

In FY 1984, ISOO became increasingly concerned about the phenomenon of "prestige" classification. This may occur when the director of a program with national security implications decides that the prestige of the program is elevated by classifying all or portions of it. Even in a properly classified program, the "prestige" phenomenon may result in the decision to overgrade the information, or to establish an unnecessary special access program. Agency oversight is critical to curbing overclassification. Managers who do not demonstrate restraint in the classification process should be relieved of this critical responsibility.

(d) Disregard of the portion marking requirements of E.O. 12356 continues to be a problem. The Order requires all classified documents to be marked to indicate which portions are classified and the level of classification. While agency heads may waive the requirement in certain situations, portion marking is especially important for information that is transmitted outside the originating office or for information that serves as a potential source of derivative classification. While most agencies and officials adhere to the rules on portion marking, some continue to transmit classified documents that have no portion markings. A result may be the unnecessary proliferation of derivatively classified information.

Classifiers most often excuse their lack of portion markings on the basis that they are "too busy" to bother with them. ISOO does not accept this. The time saved by failing to portion mark in the first instance is lost over and over again by persons who subsequently must deal with the information. Moreover, the fact that most classifiers, including some of the highest level officials within the executive branch, find the time to portion mark their classified documents undermines those who choose to shirk this responsibility.

FY 1984 Program Weaknesses: Statistical

(a) Because increases in classification activity are generally viewed as something to be avoided, ISOO lists the 9% derivative classification increase in FY 1984, and hence the 9% increase in total classification activity, as a program weakness. However, this requires some explanation. It is becoming increasingly clear that the current build-up of classified defense and intelligence programs is almost exclusively reflected in derivative actions based upon classification guides. A classification guide identifies information to be classified in the interest of national security, and prescribes the level and duration of classification for each identified item of information. The military services and defense agencies, which already relied heavily upon guides, are issuing additional guidance to cover new programs and weapons systems. The CIA and FBI, which largely spurned the use of guides until recently, now rely on them for the bulk of their classification decisions. As recently as FY 1982, original classification accounted for 6% of total classification activity. By FY 1984, it was down to 4%. This reduction largely reflects a radical change in the way information is classified in the intelligence agencies outside the DoD.

Despite the greater numbers of derivative decisions, the increased reliance upon classification guides presents a clear opportunity for the executive branch to gain and maintain better control of the classification and declassification processes. The issuance of a guide is an original classification action that only an authorized original classifier may discharge. Because a single guide often initiates thousands of derivative classification decisions, it is imperative that its author(s) understand its consequences. Clear thought, analysis, and presentation within a guide offers accuracy, uniformity, and control over the classification and declassification of a significant quantity of information. As guides account for more and more of the classified product, assuring their quality has become a paramount concern of those responsible for the quality of the information security system itself.

(b) Despite statistical evidence that the systematic review for declassification program may be healing, the program remains a matter of great concern. The vitality of systematic review primarily depends upon the vitality of the program within the National Archives and Records Administration, the only agency required to conduct a program. Following expressed concerns about the health of the program by the Assistant to the President for National Security Affairs, the Archivist of the United States commissioned a study that recommended increased resources and revised procedures for the systematic review process. For FY 1985, NARA is now hiring or placing additional personnel on the program. Unfortunately, budget limitations have already wiped out any further increases for FY 1986. NARA's increased systematic review product may not be evident until then.

The establishment of NARA as an independent agency raises several questions about the future of systematic review. Chief among them will be the attitude of NARA's new top management to the program and their ability to gain increased resources. ISOO believes that a viable systematic review program, assuming the continued commitment of agencies not required to participate, depends finally on NARA being able to review approximately 10 million pages of classified documents annually. Achieving that level remains questionable.

Conclusion

In its second full year of operation, the information security system established by E.O. 12356 remained healthy and stable. There was widespread satisfaction with the system within the executive branch and little turbulence outside. Responsible officials and employees demonstrated greater familiarity with the system in FY 1984, and their performance generally reflected that knowledge.

At the same time, however, information security remains, as always, a vulnerable system. Its credibility is constantly subject to challenge, through unauthorized disclosures, unwarranted classifications, or otherwise. The system requires vigilance. It also requires the continued support of top officials from the President on down. The information security system under E.O. 12356 has received that support. It must continue to receive it.

Appendix
ISOO Inspections: FY 1983 and 1984

AGENCY FOR INTERNATIONAL DEVELOPMENT

Bureau for Africa
Bureau for Asia
Office of Security

ARMS CONTROL AND DISARMAMENT AGENCY

Office of Administration
Communications Section
Strategic Programs Bureau
General Advisory Commission on Arms Control
Bureau of Multilateral Affairs

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

DEFENSE COMMUNICATIONS AGENCY

DEFENSE CONTRACT AUDIT AGENCY

DEFENSE INTELLIGENCE AGENCY

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

DEFENSE INVESTIGATIVE SERVICE

DEFENSE LOGISTICS AGENCY

Headquarters
Defense Technical Information 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

DEPARTMENT OF AGRICULTURE

DEPARTMENT OF THE AIR FORCE

Assistant Chief of Staff, Intelligence
Assistant Chief of Staff, Information Systems
Deputy Chief of Staff, Plans and Programs
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 Air Force Base)
Electronics Systems Division (Hanscom Air Force Base)
Aerospace Systems Division (Wright-Patterson AFB)
Foreign Technology Division (Wright-Patterson AFB)
Air Force Logistics Command Headquarters (Wright-Patterson 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, Ala.
Ballistic Missile Defense Systems Command, Huntsville, Ala.
U. S. Army Missile Command, Huntsville, Ala.
Communications - Electronics Command, Ft. Monmouth, N.J.
U. S. Army Natick Research and Development Command, Natick, Mass.
Army Materials and Mechanics Research Center, Watertown, Mass.
White Sands Missile Range, Las Cruces, New Mexico

DEPARTMENT OF COMMERCE

Headquarters' Office of Security
National Telecommunications and Information Administration
International Trade Administration

DEPARTMENT OF EDUCATION

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 Security and Safeguards

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary
Food and Drug Administration
National Institutes of Health

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

DEPARTMENT OF THE INTERIOR

Headquarters' Office of Security
U. S. Geological Survey
Bureau of Mines

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, R.I.
Naval Underwater Systems Center, Newport, R.I.
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, U.S. Atlantic Fleet, Norfolk, Va.
Headquarters Fleet Marine Force Atlantic, Norfolk, Va.
Commander Submarine Force, U.S. Atlantic Fleet, Norfolk, Va.

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

DEPARTMENT OF TRANSPORTATION

Office of the Secretary
Federal Aviation Administration
United States Coast Guard (Headquarters, Miami, New Orleans)
Maritime Commission

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

EXECUTIVE OFFICE OF THE PRESIDENT, OFFICE OF ADMINISTRATION

EXPORT IMPORT BANK

FARM CREDIT ADMINISTRATION

FEDERAL COMMUNICATIONS COMMISSION

FEDERAL EMERGENCY MANAGEMENT AGENCY

FEDERAL HOME LOAN BANK BOARD

FEDERAL MARITIME COMMISSION

FEDERAL RESERVE SYSTEM

GENERAL SERVICES ADMINISTRATION

INTERNATIONAL TRADE COMMISSION

INTERSTATE COMMERCE COMMISSION

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

NATIONAL ARCHIVES AND RECORDS SERVICE

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
Division of Security
Rules and Records Division
Records Services Branch
Standardization and Special Projects Branch

OFFICE FOR MICRONESIAN STATUS NEGOTIATIONS
OFFICE OF MANAGEMENT AND BUDGET
OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
OFFICE OF THE SECRETARY OF DEFENSE

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
Intelligence Oversight
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
Plans, Analysis and Evaluation
Defense Security Assistance Agency
Assistant to the Secretary of Defense for Atomic Energy

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, Fla.
United States Central Command, Tampa, Fla.

OVERSEAS PRIVATE INVESTMENT CORPORATION

PEACE CORPS

PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD

PRESIDENT'S INTELLIGENCE OVERSIGHT BOARD

SMALL BUSINESS ADMINISTRATION

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

UNITED STATES POSTAL SERVICE

Office of the Chief Postal Inspector
Inspection Service

VETERANS ADMINISTRATION

