

FOIA MARKER

This is not a textual record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

Collection/Record Group: Clinton Presidential Records

Subgroup/Office of Origin: Counsel Office

Series/Staff Member: Chris Cerf

Subseries:

OA/ID Number: 6975

FolderID:

Folder Title:

Personnel Security Miscellaneous : Security [2]

Stack:

S

Row:

107

Section:

2

Shelf:

11

Position:

2

Cross-Cutting and Policy Issues

ISSUE: White House Travel Office

Background

The White House Travel Office has two primary functions - arranging official commercial travel for staff of the Executive Office of the President and arranging charters for the White House press corps. Several million dollars a year flow through this office from the press corps for reimbursement of expenses related to charters.

Management reviews

During the month of May, a review of current operations was made in the Travel Office. This review substantiated many of the concerns that the management of the Travel Office was seriously deficient due to unaccounted funds, lack of financial controls, poor cash management, lack of documentation, and no formal financial reporting process for the financial activities of the office. On May 19, 1993, the seven employees of the White House Travel Office were dismissed.

On May 25, 1993, a second review was made to review the dismissal of the seven employees. The review was conducted with the assistance of the Office of Management and Budget (OMB); a separate financial audit by the public accounting firm of KPMG Peat Marwick was also performed. The General Accounting Office (GAO) is currently conducting a review of the Travel Office that is not completed.

NPR Connection

In conjunction with the financial audit, the NPR team, responsible for the NPR management reviews within the EOP, *accompanied* the Peat Marwick audit team in reviewing the Travel Office. The NPR team was responsible for reviewing management practices within each agency of the EOP, including the White House Office, and was responsible for incorporating recommendations for the EOP agencies into the NPR report, which was released September 7, 1993. The National Performance Review (NPR) did not include any recommendations for the White House Travel Office. [Note: Peat Marwick was recommended by "an Office of Administration assistant" who had attended a seminar given by Peat Marwick under the auspices of the National Performance Review.]

Interim arrangements

World Wide Travel began operations in the White House Travel Office, on May 19, 1993, immediately after the former staff was dismissed to handle commercial travel for an interim period. Their services, for which no payment has been made, were rendered for one Presidential trip to New Hampshire on May 22, 1993. After this trip, a mutual agreement was reached that World Wide Travel would cease operations in the Travel Office, due to the appearance of favoritism in using the firm. A purchase order, not to exceed \$2,500 of FY 1993 funds, was executed to provide payment to World Wide once all investigations have been completed favorably and a determination can be made on the amount due the firm.

Management improvements

On May 24, 1993, a competitive contract was awarded through GSA to the American Express Co. to set up a Travel Management Center (TMC) in the Old Executive Office Building. After the TMC was established, the staff from American Express issued all the commercial transportation tickets, and GSA assisted in arranging press travel until a director for the White House Travel Office could be brought on board. Also, based on data compiled since May 1993, the use of competitive bidding for press travel has resulted in savings of approximately \$127,000 in charters arranged between May and October. This amount represents a savings of 24% less than what costs would have been using the former pricing scenario.

Current status

Currently, the Travel Office consists of four White House Office employees who are paid less than the previous employees. The employees are: Steve Reiwerts, Director; Kim Johnson, Assistant Director; Ashley Adams, Trip Coordinator and Chris Enskov, Trip Coordinator.

Five of the former Travel Office employees who were dismissed and who had no financial management responsibilities were reinstated to similar positions in other Federal agencies; two other employees filed for retirement.

Congress included funds for the payment of legal fees for the five non-management employees of the Travel Office in the appropriation for the Department of Transportation (DOT) in November 1993. The DOT General Counsel is dealing directly with the attorneys representing the former Travel Office employees regarding the legal fees. Inquiries on this subject should be directed to DOT.

Cross-Cutting and Policy Issues

ISSUE: ***Office of National Service***

Background

Treasury/Postal Committee

Senate reduced WHO by 1 FTE and \$160,000 to fund the Office of National Service (ONS) under the VA/HUD bill. WHO appropriation was passed with the \$160,000 reduction.

VA/HUD Committee

Senate report recommended funding ONS at \$160,000 and within the Office of Administration within the EOP. The VA/HUD Conference Committee limited reimbursement for detailees to \$50,000, and ONS must pay no less than 50% for all detailees. Public Law 103-124, VA/HUD Appropriations, specifically addressed the reimbursement of detailees.

Mission & Duties

Established to implement and oversee the National and Community Service Act of 1990. The Office formulates and coordinates executive branch policy on national service including liaison with private and public sector organizations such as the Points of Light Foundation [source: VA/HUD Appropriations Senate Report].

Action

The Office of National Service will fund 4 reimbursable detailees within its budget. Through pay period Z, ending December 18, 1993, ONS reached the \$50,000 limit for 4 detailees. Mr. Jacob Lew from WHO was transferred to ONS to fill the FTE slot. The \$160,000 budget is being used to fund personnel compensation only. Mr. Lew is classified as a consultant.

Fiscal Year 1995

The White House Office has not requested funding for the Office of National Service in FY 1995. **Update: Why not?**

Codification of Presidential Proclamations and Executive Orders

(1989)

(1) Payments shall begin as of the date of arrival at the post on assignment or transfer and shall end as of the date of departure from the post for separation or transfer, except that in case of local recruitment such payments shall begin and end as of the beginning and end of employment, respectively.

(2) Payments for periods of leave and of detail shall begin and end as determined in regulations prescribed under section 202(c) hereof.

(3) Payments to persons serving on a part-time basis shall be prorated to cover only those periods of time for which such persons receive basic compensation.

(4) Payment shall not be made for any time for which an employee does not receive basic compensation.

(b) Non-foreign area post differentials paid shall not be included in the base used in computing overtime pay, night differential, holiday pay, and retirement deduction.

[Sec. 208 amended by EO 10635 of Sept. 16, 1955, 3 CFR, 1954-1958 Comp., p. 268; EO 12510 of Apr. 17, 1985, 50 FR 15535, 3 CFR, 1985 Comp., p. 338]

SEC. 209. *Persons serving under contract.* Any other provision of this Part notwithstanding, any person who would otherwise be eligible to receive a non-foreign area post differential or a non-foreign area cost-of-living allowance under this Part shall, if he is serving under a contract, be compensated according to the terms of such contract for the period thereof and shall, during such period, be ineligible to receive said differential and allowance.

[Sec. 209 amended by EO 12510 of Apr. 17, 1985, 50 FR 15535, 3 CFR, 1985 Comp., p. 338]

SEC. 210. *Periodic review.* The Office of Personnel Management shall periodically, but at least annually, review the places designated, the rates fixed, and the regulations prescribed pursuant to this Part, with a view to making such changes therein as will insure that payment of additional compensation under the provisions of this Part shall continue only during the continuance of conditions justifying such payment and shall not in any instance exceed the amount justified: *Provided*, That if program or methodology revisions would substantially reduce an established differential or allowance rate, then the rate of such additional compensation may be reduced gradually.

[Sec. 210 amended by EO 11938 of Sept. 29, 1976, 41 FR 43383, 3 CFR, 1976 Comp., p. 148; EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

PART III—INTERIM ARRANGEMENTS

[Part III revoked by EO 10903 of Jan. 9, 1961, 26 FR 217, 3 CFR, 1959-1963 Comp., p. 433]

PART IV—FOREIGN SERVICE SALARY DIFFERENTIALS

[Part IV revoked by EO 10903 of Jan. 9, 1961, 26 FR 217, 3 CFR, 1959-1963 Comp., p. 433]

Chapter 5—Federal Civilian Personnel

PART V—UNHEALTHFUL POSTS

[Part V revoked by EO 10903 of Jan. 9, 1961, 26 FR 217, 3 CFR, 1959-1963 Comp., p. 433]

PART VI—GENERAL PROVISIONS

SEC. 601. *Publication.* This order, and the places designated, the rates fixed, and the regulations prescribed by the Secretary of State and the Office of Personnel Management pursuant to Parts I and II of this order, shall be published in the FEDERAL REGISTER.

[Sec. 601 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Executive Order 10450—Security requirements for Government employment

SOURCE: The provisions of Executive Order 10450 of Apr. 27, 1953, appear at 18 FR 2489, 3 CFR, 1949-1953 Comp., p. 936, unless otherwise noted.

WHEREAS the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and

WHEREAS the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service:

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U.S.C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U.S.C. 632, *et seq.*); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U.S.C. 118j); and the act of August 26, 1950, 64 Stat. 476 (5 U.S.C. 22-1, *et seq.*), and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

SECTION 1. In addition to the departments and agencies specified in the said act of August 26, 1950, and Executive Order No. 10237 of April 26, 1951, the provisions of that act shall apply to all other departments and agencies of the Government.¹

SEC. 2. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

¹ EDITORIAL NOTE: In *Cole v. Young*, 76 S.Ct. 861 (1955), section 1 of EO 10450 was held to be invalid if applied to every department and agency.

SEC. 3. (a) The appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation. The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation: *Provided*, that upon request of the head of the department or agency concerned, the Office of Personnel Management may, in its discretion, authorize such less investigation as may meet the requirements of the national security with respect to per-diem, intermittent, temporary, or seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, there shall be conducted with respect to such person a full field investigation, or such less investigation as shall be sufficient to enable the head of the department or agency concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

(b) The head of any department or agency shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full field investigation has been conducted: *Provided*, that a person occupying a sensitive position at the time it is designated as such may continue to occupy such position pending the completion of a full field investigation, subject to the other provisions of this order: *And provided further*, that in case of emergency a sensitive position may be filled for a limited period by a person with respect to whom a full field pre-appointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

[Sec. 3 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 4. The head of each department and agency shall review, or cause to be reviewed, the cases of all civilian officers and employees with respect to whom there has been conducted a full field investigation under Executive Order No. 9835 of March 21, 1947, and, after such further investigation as may be appropriate, shall re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, such of those cases as have not been adjudicated under a security standard commensurate with that established under this order.

SEC. 5. Whenever there is developed or received by any department or agency information indicating that the retention in employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his

representative, who, after such investigation as may be appropriate, shall review, or cause to be reviewed, and, where necessary, re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, the case of such officer or employee.

SEC. 6. Should there develop at any stage of investigation information indicating that the employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, the head of the department or agency concerned or his representative shall immediately suspend the employment of the person involved if he deems such suspension necessary in the interests of the national security and, following such investigation and review as he deems necessary, the head of the department or agency concerned shall terminate the employment of such suspended officer or employee whenever he shall determine such termination necessary or advisable in the interests of the national security, in accordance with the said act of August 26, 1950.

SEC. 7. Any person whose employment is suspended or terminated under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950, or pursuant to the said Executive Order No. 9835 or any other security or loyalty program relating to officers or employees of the Government, shall not be reinstated or restored to duty or reemployed in the same department or agency and shall not be reemployed in any other department or agency, unless the head of the department or agency concerned finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of the national security, which finding shall be made a part of the records of such department or agency: *Provided*, that no person whose employment has been terminated under such authority thereafter may be employed by any other department or agency except after a determination by the Office of Personnel Management that such person is eligible for such employment.

[Sec. 7 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 8. (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:

(1) Depending on the relation of the Government employment to the national security:

(i) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

(ii) Any deliberate misrepresentations, falsifications, or omissions of material facts.

(iii) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, sexual perversion.

(iv) Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.

(v) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.

(2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereof or preparation therefor, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(3) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

(4) Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

(5) Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons (hereinafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State, or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.

(6) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(7) Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(8) Refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of his alleged disloyalty or other misconduct.

(b) The investigation of persons entering or employed in the competitive service shall primarily be the responsibility of the Office of Personnel Management, except in cases in which the head of a department or agency assumes that responsibility pursuant to law or by agreement with the Office. The Office shall furnish a full investigative report to the department or agency concerned.

(c) The investigation of persons (including consultants, however employed), entering employment of, or employed by, the Government other than in the competitive service shall primarily be the responsibility of the employing department or agency. Departments and agencies without investigative facilities may use the investigative facilities of the Office of Personnel Management, and other departments and agencies may use such facilities under agreement with the Office.

(d) There shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests

of the national security, or information relating to any of the matters described in subdivisions (2) through (8) of subsection (a) of this section. In cases so referred to it, the Federal Bureau of Investigation shall make a full field investigation.

[Sec. 8 amended by EO 10491 of Oct. 13, 1953, 18 FR 6583, 3 CFR, 1949-1953 Comp., p. 973; EO 10531 of May 27, 1954, 19 FR 3069, 3 CFR, 1954-1958 Comp., p. 193; EO 10548 of Aug. 2, 1954, 19 FR 4871, 3 CFR, 1954-1958 Comp., p. 200; EO 11785 of June 4, 1974, 39 FR 20053, 3 CFR, 1971-1975 Comp., p. 874; EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 9. (a) There shall be established and maintained in the Office of Personnel Management a security-investigations index covering all persons as to whom security investigations have been conducted by any department or agency of the Government under this order. The central index established and maintained by the Office under Executive Order No. 9835 of March 21, 1947, shall be made a part of the security-investigations index. The security-investigations index shall contain the name of each person investigated, adequate identifying information concerning each such person, and a reference to each department and agency which has conducted an investigation concerning the person involved or has suspended or terminated the employment of such person under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950.

(b) The heads of all departments and agencies shall furnish promptly to the Office of Personnel Management information appropriate for the establishment and maintenance of the security-investigations index.

(c) The reports and other investigative material and information developed by investigations conducted pursuant to any statute, order, or program described in section 7 of this order shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with the said act of August 26, 1950, as may be required for the efficient conduct of Government business.

[Sec. 9 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 10. Nothing in this order shall be construed as eliminating or modifying in any way the requirement for any investigation or any determination as to security which may be required by law.

SEC. 11. On and after the effective date of this order the Loyalty Review Board established by Executive Order No. 9835 of March 21, 1947, shall not accept agency findings for review, upon appeal or otherwise. Appeals pending before the Loyalty Review Board on such date shall be heard to final determination in accordance with the provisions of the said Executive Order No. 9835, as amended. Agency determinations favorable to the officer or employee concerned pending before the Loyalty Review Board on such date shall be acted upon by such Board, and whenever the Board is not in agreement with such favorable determination the case shall be remanded to the department or agency concerned for determination in accordance with the standards

and procedures established pursuant to this order. Cases pending before the regional loyalty boards of the Office of Personnel Management on which hearings have not been initiated on such date shall be referred to the department or agency concerned. Cases being heard by regional loyalty boards on such date shall be heard to conclusion and the determination of the board shall be forwarded to the head of the department or agency concerned: *Provided*, that if no specific department or agency is involved, the case shall be dismissed without prejudice to the applicant. Investigations pending in the Federal Bureau of Investigation or the Office of Personnel Management on such date shall be completed, and the reports thereon shall be made to the appropriate department or agency.

[Sec. 11 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 12. Executive Order No. 9835 of March 21, 1947, as amended, is hereby revoked.

[Sec. 12 amended by EO 11785 of June 4, 1974, 39 FR 20053, 3 CFR, 1971-1975 Comp., p. 874]

SEC. 13. The Attorney General is requested to render to the heads of departments and agencies such advice as may be requisite to enable them to establish and maintain an appropriate employee-security program.

SEC. 14. (a) The Office of Personnel Management, with the continuing advice and collaboration of representatives of such departments and agencies as the National Security Council may designate, shall make a continuing study of the manner in which this order is being implemented by the departments and agencies of the Government for the purpose of determining:

(1) Deficiencies in the department and agency security programs established under this order which are inconsistent with the interests of, or directly or indirectly weaken, the national security.

(2) Tendencies in such programs to deny to individual employees fair, impartial, and equitable treatment at the hands of the Government, or rights under the Constitution and laws of the United States or this order.

Information affecting any department or agency developed or received during the course of such continuing study shall be furnished immediately to the head of the department or agency concerned. The Office of Personnel Management shall report to the National Security Council, at least semiannually, on the results of such study, shall recommend means to correct any such deficiencies or tendencies, and shall inform the National Security Council immediately of any deficiency which is deemed to be of major importance.

(b) All departments and agencies of the Government are directed to cooperate with the Office of Personnel Management to facilitate the accomplishment of the responsibilities assigned to it by subsection (a) of this section.

(c) To assist the Office of Personnel Management in discharging its responsibilities under this order, the head of each department and agency shall, as soon as possible and in no event later than ninety days after receipt of the final investigative report on a civilian officer or employee subject to a full field investigation under the provisions of this

order, advise the Office as to the action taken with respect to such officer or employee. The information furnished by the heads of departments and agencies pursuant to this section shall be included in the reports which the Office of Personnel Management is required to submit to the National Security Council in accordance with subsection (a) of this section. Such reports shall set forth any deficiencies on the part of the heads of departments and agencies in taking timely action under this order, and shall mention specifically any instances of noncompliance with this subsection.

[Sec. 14 amended by EO 10550 of Aug. 5, 1954, 19 FR 4981, 3 CFR, 1954-1958 Comp., p. 200; EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

SEC. 15. This order shall become effective thirty days after the date hereof.

Executive Order 10471—Authorizing the heads of departments and agencies to grant leaves of absence to certain persons

SOURCE: The provisions of Executive Order 10471 of July 17, 1953, appear at 18 FR 4231, 3 CFR, 1949-1953 Comp., p. 952, unless otherwise noted.

By virtue of the authority vested in me by section 301 of title 3 of the United States Code, and as President of the United States, if is ordered as follows:

1. The heads of the several departments and agencies of the Government are hereby authorized and empowered, without the approval, ratification, or other action of the President, to exercise, with respect to personnel in their respective department or agency, the authority conferred upon the President by section 6305(b) of title 5 of the United States Code, to authorize leaves of absence in accordance with the said section 6305(b) to persons who receive compensation in accordance with section 401 of the Foreign Service Act of 1980 (22 U.S.C. 3961).

[Sec. 1 amended by EO 12292 of Feb. 23, 1981, 46 FR 13967, 3 CFR, 1981 Comp., p. 134]

2. This order shall be effective as of July 5, 1953.

Executive Order 10552—Delegating to the Office of Personnel Management the authority of the President to promulgate regulations under which certain Government employees may be prevented or relieved from working by administrative order

SOURCE: The provisions of Executive Order 10552 of Aug. 10, 1954, appear at 19 FR 5079, 3 CFR, 1954-1958 Comp., p. 201, unless otherwise noted.

By virtue of the authority vested in me by section 301 of title 3 of the United States Code, 65 Stat. 713, it is declared that the Office of Personnel Management be, and it is hereby, designated and empowered to exercise, without the approval, ratification, or other action of the President, the authority vested in the President by the joint resolution of June 29, 1938, 52 Stat. 1246, as amended by the act of June 11, 1954, 68 Stat. 249 (5 U.S.C. 86a), to promulgate regulations under which certain employees of the Government may be prevented or relieved from working by administrative order.

Cross-Cutting and Policy Issues

Issue: White House Passes

Summary

The White House and the Executive Office of the President have recently come under criticism for delays in processing permanent passes. The White House has aggressively investigated the issue and has already implemented procedures:

- (1) to reinforce existing guidelines for insuring 100% compliance by all personnel; and
- (2) to streamline and accelerate the process for completing full security checks.

Even before these steps were taken, existing practices and procedures insured that White House personnel would not have access to the Complex until they had passed a preliminary security check. That check, which occurs before issuance of even a temporary pass, satisfies one of the principal objectives of a background investigation: minimizing the risk that dangerous or unstable individuals would have access to the White House Complex.

Current Statistics

White House

Of the 493 individuals in the White House (defined for these purposes to include OVP and OPD):

- 239 have permanent passes;
- 165 have favorably adjudicated background investigations (BIs);
- 67 have BI's pending;
- 22 have not yet completed the paperwork

All of the employees who have not completed their preliminary paperwork are now in compliance with the Chief of Staff's directive that all staff must complete the requisite forms within 30 days of beginning work.

The NSC

Of the 153 individuals working for the NSC:

- 87 have permanent passes;
- 37 have favorably adjudicated BIs;
- 22 have BI's pending;
- 7 have not yet completed paperwork

All of the individuals who have not submitted the required paperwork are in compliance with the Chief of Staff's thirty-day rule.

Other Components of the EOP (Excluding OMB and USTR)

Attachment 1, prepared by Chuck Easley, summarizes the status of other EOP components. Note that all employees have submitted the necessary paperwork.

Statistical Overview

1. Of the over 1000 employees working in the White House or one of the EOP components detailed above, all but 29 have completed the necessary paperwork.

2. All of these 29 individuals have been employed for less than 30 days and are therefore in compliance with the COS's directive.

3. All current employees have been the subject of -- and passed -- a preliminary background check, which includes an FBI (NCIC) computer search for criminal history and a review of any existing intelligence files previously maintained on the individual.

4. With no or virtually no exceptions, all employees who have been in complex for 30 days or more have also submitted to fingerprint testing, which is immediately submitted for further evaluation by the FBI.

General Procedures

White House

[

**EXECUTIVE OFFICE OF THE PRESIDENT
SECURITY CLEARANCE / PASS STATISTICS**

16-Mar-94 17:29

AGENCY	Number of Staff incl detailees	No. of Passes Issued	No. of Temp WH Passes	No. of Temp QEOB Passes	Adjudicated Backgrounds Completed	Pending Background Investigations	Awaiting Paperwork
White House Office	425	194			109	93	23
Office of Policy Development	52	8	10	2			0
Council on Environmental Quality	6	6	0	1	0	1	0
Executive Residence	89	89	0	0	0	0	0
Office of the Vice President	26	13			9	0	2
Residence of the Vice President	1	0	0	0	0	0	0
National Security Council	149	92	55	19	41	28	5
Office of Nat'l Drug Control Policy	23	18	1	3	1	3	0
Office of Science & Tech Policy	42	25	10	6	10	6	0
Council of Economic Advisers	35	28	3	3	3	3	0
Office of Administration	185	177	5	3	5	3	0
TOTAL	1033	650	84	37	178	137	30

Procedures for Hiring and Obtaining Access for New Employees

DRAFT

Administrative Contact for employing department submits the following completed forms to the Office of Management and Administration. These forms are available from Room 145:

- a. *Pre-employment Form*, completed by administrative contact and signed by the Assistant to the President for that department;
 - b. *Drug Testing Form*, completed and signed by the prospective employee and
 - c. *Supplemental Personnel Form ("blue form")* with appropriate sections completed by the administrative contact and the prospective employee and signed by the department head and the prospective employee.
2. Management and Administration coordinates with White House Personnel Security to schedule and conduct security interview.
 3. Management and Administration coordinates with the Office of Administration, Personnel Management Division to have prospective employee tested for illegal drug use.
 4. Upon conclusion of security interview and favorable recommendation from Security, Management and Administration approves *Pre-employment Form* and notifies administrative contact for employing department accordingly.
 5. Management and Administration sends security packet to administrative contact for prospective employee's department completion by prospective employee.
 6. Management and Administration approves the *Supplemental Personnel Form*¹ and sends it to White House Personnel Security for action. Effective date of hire is noted as "Effective Date" on the *blue form*. Management and Administration may make changes to the *blue form* regarding personnel status, or effective date, if necessary.
 7. White House Personnel Security initiates the FBI name check and other investigatory procedures.
 8. New employee has 30 days from **effective date of hire** to submit completed security forms (SF-86, FBI consent, tax check waiver, personal data statement questionnaire, and other required forms) to White House Personnel Security.
 9. If new employee has not submitted security forms within the 30-day time frame, White House Personnel Security will first notify Management and Administration. Management and Administration will take the necessary steps to place the employee in a Leave Without Pay status. Next, Security will take the necessary steps to revoke the individual's access to the Complex.

¹Approval by White House Management and Administration indicates only that the individual has been selected for employment and authorizes White House Personnel Security to initiate an FBI name check and other investigatory procedures.

DRAFT

USSS SENATE APPROPRIATION HEARING

- March 11, 1994, 10:00 A.M.
- Senators in attendance were DeConcini and Bond
- Also in attendance were representatives from USSS as well as US Treasury Department
- After the opening remarks, DeConcini lead with a question about the White House pass issue. He said that USSS has been given money specifically to enhance the access system. "With all of this mess in the news, whose fault is it that these passes are not being given out?" The Director of the Secret Service then explained the process of issuing a pass.
 1. WH identifies an individual
 2. FBI conducts a background investigation
 3. Results are then turned over to the WH for their review and they are then responsible for getting the proper paperwork done (ie, Tax Release Waiver forms, ect.).
 4. After all the necessary data is gathered, USSS receives the information back from the WH. USSS then reviews the information and makes a recommendation to the WH whether the individual in question should be given access to the WH.
 5. WH makes the final decision as to if the individual will receive a building pass.
- DeConcini asked where the hold up was. USSS said to their knowledge, the hold up is on WH's end. At this point, the representative for Treasury interjected that he thinks that two issues are being combined that are really separate (implying the media has gone on a wrong assumption). Access to the WH has nothing to do with security clearances. "Just because someone has access to the WH does not mean that they have access to secret documents."
- Senator Bond then said "Is the only hold up that information has not been given to the USSS? Is there any instant where you have decided to not recommend someone receive a pass?" The Director responded that USSS does make recommendations, but it is ultimately the WH that decides who will receive a pass. The USSS made it clear that they have very little power to deny passes. They simply provide the information to the WH with their recommendations. Senator DeConcini made the point that USSS is only concerned with the security of the building. Another member of the USSS reminded the Senators that prior to getting a temporary badge, you do have to pass an initial background check.

- Bond asked if there were any individuals that the USSS recommended not being given a pass that where then in fact given a pass by the WH anyway. The USSS said not to their immediate knowledge, but they would have to check to make sure.
- During the proceedings, Bond offered an extreme hypothetical of a person who was a child molester and a mad-man and asked if he would indeed not be recommended to receive a pass. The USSS said that they probably would not recommend that individual receive a pass. Bond ask later about drug use, but the representative from Treasury objected. He said that he would discuss in private, reasons for not recommending a person for a pass, but he would rather not discuss it at an open hearing.
- Then the rumor that a large number of passes that have been issued in the recent number of weeks or days was discussed. The Director of USSS said that he did not have that information available but would provide it at a later date. Bond then asked if they have ever pulled a pass. The USSS agreed that they have in the past pulled persons passes.
- Bond then got a little more specific and asked if they had done so in the last few years. The USSS has revoked passes in the last few years. DeConcini said, "Just ask. Have you had to do this in the last 14 months?" The director responded no, and that if the senators would like to hear reasons that a pass may be pulled they would be willing to talk about that in a private meeting. The senators then went on to other business.

Presidential Documents

Title 3—

The President

Executive Order 12829 of January 6, 1993

National Industrial Security Program

This order establishes a National Industrial Security Program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. To promote our national interests, the United States Government issues contracts, licenses, and grants to nongovernment organizations. When these arrangements require access to classified information, the national security requires that this information be safeguarded in a manner equivalent to its protection within the executive branch of Government. The national security also requires that our industrial security program promote the economic and technological interests of the United States. Redundant, overlapping, or unnecessary requirements impede those interests. Therefore, the National Industrial Security Program shall serve as a single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests.

Therefore, by the authority vested in me as President by the Constitution and the laws of the United States of America, including the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011-2286), the National Security Act of 1947, as amended (codified as amended in scattered sections of the United States Code), and the Federal Advisory Committee Act, as amended (5 U.S.C. App. 2), it is hereby ordered as follows:

PART 1. ESTABLISHMENT AND POLICY

Section 101. *Establishment.* (a) There is established a National Industrial Security Program. The purpose of this program is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies. For the purposes of this order, the terms "contractor, licensee, or grantee" means current, prospective, or former contractors, licensees, or grantees of United States agencies. The National Industrial Security Program shall be applicable to all executive branch departments and agencies.

✓ (b) The National Industrial Security Program shall provide for the protection of information classified pursuant to Executive Order No. 12356 of April 2, 1982, or its successor, and the Atomic Energy Act of 1954, as amended.

(c) For the purposes of this order, the term "contractor" does not include individuals engaged under personal services contracts.

Sec. 102. *Policy Direction.* (a) The National Security Council shall provide overall policy direction for the National Industrial Security Program.

✓ (b) The Director of the Information Security Oversight Office, established under Executive Order No. 12356 of April 2, 1982, shall be responsible for implementing and monitoring the National Industrial Security Program and shall:

(1) develop, in consultation with the agencies, and promulgate subject to the approval of the National Security Council, directives for the implementation of this order, which shall be binding on the agencies;

(2) oversee agency, contractor, licensee, and grantee actions to ensure compliance with this order and implementing directives;

(3) review all agency implementing regulations, internal rules, or guidelines. The Director shall require any regulation, rule, or guideline to be changed if it is not consistent with this order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation, rule, or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority, pursuant to terms of applicable contracts, licenses, grants, or regulations, to conduct on-site reviews of the implementation of the National Industrial Security Program by each agency, contractor, licensee, and grantee that has access to or stores classified information and to require of each agency, contractor, licensee, and grantee those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific classified information, or other forms of cooperation, would pose an exceptional national security risk, the affected agency head or the senior official designated under section 203(a) of this order may request the National Security Council to deny access to the Director. The Director shall not have access pending a prompt decision by the National Security Council;

(5) report any violations of this order or its implementing directives to the head of the agency or to the senior official designated under section 203(a) of this order so that corrective action, if appropriate, may be taken. Any such report pertaining to the implementation of the National Industrial Security Program by a contractor, licensee, or grantee shall be directed to the agency that is exercising operational oversight over the contractor, licensee, or grantee under section 202 of this order;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the National Industrial Security Program;

(7) consider, in consultation with the advisory committee established by this order, affected agencies, contractors, licensees, and grantees, and recommend to the President through the National Security Council changes to this order; and

(8) report at least annually to the President through the National Security Council on the implementation of the National Industrial Security Program.

(c) Nothing in this order shall be construed to supersede the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended, or the authority of the Director of Central Intelligence under the National Security Act of 1947, as amended, or Executive Order No. 12333 of December 8, 1981.

Sec. 103. National Industrial Security Program Policy Advisory Committee.

(a) *Establishment.* There is established the National Industrial Security Program Policy Advisory Committee ("Committee"). The Director of the Information Security Oversight Office shall serve as Chairman of the Committee and appoint the members of the Committee. The members of the Committee shall be the representatives of those departments and agencies most affected by the National Industrial Security Program and nongovernment representatives of contractors, licensees, or grantees involved with classified contracts, licenses, or grants, as determined by the Chairman.

(b) *Functions.* (1) The Committee members shall advise the Chairman of the Committee on all matters concerning the policies of the National Industrial Security Program, including recommended changes to those policies as reflected in this order, its implementing directives, or the operating manual established under this order, and serve as a forum to discuss policy issues in dispute.

(2) The Committee shall meet at the request of the Chairman, but at least twice during the calendar year.

(c) *Administration.* (1) Members of the Committee shall serve without compensation for their work on the Committee. However, nongovernment members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5701-5707).

(2) To the extent permitted by law and subject to the availability of funds, the Administrator of General Services shall provide the Committee with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(d) *General.* Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, except that of reporting to the Congress, which are applicable to the Committee, shall be performed by the Administrator of General Services in accordance with the guidelines and procedures established by the General Services Administration.

PART 2. OPERATIONS

Sec. 201. National Industrial Security Program Operating Manual. (a) The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, and the Director of Central Intelligence, shall issue and maintain a National Industrial Security Program Operating Manual ("Manual"). The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe and issue that portion of the Manual that pertains to information classified under the Atomic Energy Act of 1954, as amended. The Director of Central Intelligence shall prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information.

(b) The Manual shall prescribe specific requirements, restrictions, and other safeguards that are necessary to preclude unauthorized disclosure and control authorized disclosure of classified information to contractors, licensees, or grantees. The Manual shall apply to the release of classified information during all phases of the contracting process including bidding, negotiation, award, performance, and termination of contracts, the licensing process, or the grant process, with or under the control of departments or agencies.

(c) The Manual shall also prescribe requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including Restricted Data, Formerly Restricted Data, intelligence sources and methods information, Sensitive Compartmented Information, and Special Access Program Information.

(d) In establishing particular requirements, restrictions, and other safeguards within the Manual, the Secretary of Defense, the Secretary of Energy, the Nuclear Regulatory Commission, and the Director of Central Intelligence shall take into account these factors: (i) the damage to the national security that reasonably could be expected to result from an unauthorized disclosure; (ii) the existing or anticipated threat to the disclosure of information; and (iii) the short- and long-term costs of the requirements, restrictions, and other safeguards.

(e) To the extent that is practicable and reasonable, the requirements, restrictions, and safeguards that the Manual establishes for the protection of classified information by contractors, licensees, and grantees shall be consistent with the requirements, restrictions, and safeguards that directives implementing Executive Order No. 12356 of April 2, 1982, or the Atomic Energy Act of 1954, as amended, establish for the protection of classified information by agencies. Upon request by the Chairman of the Committee, the Secretary of Defense shall provide an explanation and justification for any requirement, restriction, or safeguard that results in a standard for

the protection of classified information by contractors, licensees, and grantees that differs from the standard that applies to agencies.

(f) The Manual shall be issued no later than 1 year from the issuance of this order.

Sec. 202. Operational Oversight. (a) The Secretary of Defense shall serve as Executive Agent for inspecting and monitoring the contractors, licensees, and grantees who require or will require access to, or who store or will store classified information; and for determining the eligibility for access to classified information of contractors, licensees, and grantees and their respective employees. The heads of agencies shall enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on behalf of these agency heads.

(b) The Director of Central Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of Central Intelligence may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, to inspect and monitor these programs or facilities, in whole or in part, on the Director's behalf.

(c) The Secretary of Energy and the Nuclear Regulatory Commission retain authority over access to information under their respective programs classified under the Atomic Energy Act of 1954, as amended. The Secretary or the Commission may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, to inspect and monitor these programs or facilities, in whole or in part, on behalf of the Secretary or the Commission, respectively.

(d) The Executive Agent shall have the authority to issue, after consultation with affected agencies, standard forms or other standardization that will promote the implementation of the National Industrial Security Program.

Sec. 203. Implementation. (a) The head of each agency that enters into classified contracts, licenses, or grants shall designate a senior agency official to direct and administer the agency's implementation and compliance with the National Industrial Security Program.

(b) Agency implementing regulations, internal rules, or guidelines shall be consistent with this order, its implementing directives, and the Manual. Agencies shall issue these regulations, rules, or guidelines no later than 180 days from the issuance of the Manual. They may incorporate all or portions of the Manual by reference.

(c) Each agency head or the senior official designated under paragraph (a) above shall take appropriate and prompt corrective action whenever a violation of this order, its implementing directives, or the Manual occurs.

(d) The senior agency official designated under paragraph (a) above shall account each year for the costs within the agency associated with the implementation of the National Industrial Security Program. These costs shall be reported to the Director of the Information Security Oversight Office, who shall include them in the reports to the President prescribed by this order.

(e) The Secretary of Defense, with the concurrence of the Administrator of General Services, the Administrator of the National Aeronautics and Space Administration, and such other agency heads or officials who may be responsible, shall amend the Federal Acquisition Regulation to be consistent with the implementation of the National Industrial Security Program.

(f) All contracts, licenses, or grants that involve access to classified information and that are advertised or proposed following the issuance of agency regulations, rules, or guidelines described in paragraph (b) above shall comply with the National Industrial Security Program. To the extent that is feasible, economical, and permitted by law, agencies shall amend, modify, or convert

preexisting contracts, licenses, or grants, or previously advertised or proposed contracts, licenses, or grants, that involve access to classified information for operation under the National Industrial Security Program. Any direct inspection or monitoring of contractors, licensees, or grantees specified by this order shall be carried out pursuant to the terms of a contract, license, grant, or regulation.

(g) Executive Order No. 10865 of February 20, 1960, as amended by Executive Order No. 10909 of January 17, 1961, and Executive Order No. 11382 of November 27, 1967, is hereby amended as follows:

(1) Section 1(a) and (b) are revoked as of the effective date of this order.

(2) Section 1(c) is renumbered as Section 1 and is amended to read as follows:

"Section 1. When used in this order, the term 'head of a department' means the Secretary of State, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, the Nuclear Regulatory Commission, the Administrator of the National Aeronautics and Space Administration, and, in section 4, the Attorney General. The term 'head of a department' also means the head of any department or agency, including but not limited to those referenced above with whom the Department of Defense makes an agreement to extend regulations prescribed by the Secretary of Defense concerning authorizations for access to classified information pursuant to Executive Order No. 12829."

(3) Section 2 is amended by inserting the words "pursuant to Executive Order No. 12829" after the word "information."

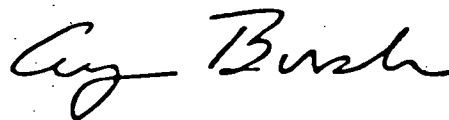
(4) Section 3 is amended by inserting the words "pursuant to Executive Order No. 12829" between the words "revoked" and "by" in the second clause of that section.

(5) Section 6 is amended by striking out the words "The Secretary of State, the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, the Secretary of Transportation, or his representative, or the head of any other department or agency of the United States with which the Department of Defense makes an agreement under section (1)(b)," at the beginning of the first sentence, and inserting in their place "The head of a department of the United States"

(6) Section 8 is amended by striking out paragraphs (1) through (7) and inserting in their place ". . . the deputy of that department, or the principal assistant to the head of that department, as the case may be."

(h) All delegations, rules, regulations, orders, directives, agreements, contracts, licenses, and grants issued under preexisting authorities, including section 1(a) and (b) of Executive Order No. 10865 of February 20, 1960, as amended, by Executive Order No. 10909 of January 17, 1961, and Executive Order No. 11382 of November 27, 1967, shall remain in full force and effect until amended, modified, or terminated pursuant to authority of this order.

(i) This order shall be effective immediately.



THE WHITE HOUSE,
January 6, 1993.

Codification of Presidential Proclamations and Executive Orders

The Board shall utilize such full-time staff and consultants as authorized by the President.

SEC. 2. The Board shall:

(a) Inform the President of intelligence activities that any member of the Board believes are in violation of the Constitution or laws of the United States, Executive orders, or Presidential directives;

(b) Forward to the Attorney General reports received concerning intelligence activities that the Board believes may be unlawful;

(c) Review the internal guidelines of each agency within the Intelligence Community concerning the lawfulness of intelligence activities;

(d) Review the practices and procedures of the Inspectors General and General Counsel of the Intelligence Community for discovering and reporting intelligence activities that may be unlawful or contrary to Executive order or Presidential directive; and

(e) Conduct such investigations as the Board deems necessary to carry out its functions under this Order.

SEC. 3. The Board shall, when required by this Order, report directly to the President. The Board shall consider and take appropriate action with respect to matters identified by the Director of Central Intelligence, the Central Intelligence Agency or other agencies of the Intelligence Community. With respect to matters deemed appropriate by the President, the Board shall advise and make appropriate recommendations to the Director of Central Intelligence, the Central Intelligence Agency, and other agencies of the Intelligence Community.

SEC. 4. The heads of departments and agencies of the Intelligence Community shall, to the extent permitted by law, provide the Board with all information necessary to carry out its responsibilities. Inspectors General and General Counsel of the Intelligence Community shall, to the extent permitted by law, report to the Board concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive.

SEC. 5. Information made available to the Board shall be given all necessary security protection in accordance with applicable laws and regulations. Each member of the Board, each member of the Board's staff, and each of the Board's consultants shall execute an agreement never to reveal any classified information obtained by virtue of his or her service with the Board except to the President or to such persons as the President may designate.

SEC. 6. Members of the Board shall serve without compensation, but may receive transportation, expense, and per diem allowances as authorized by law. Staff and consultants to the Board shall receive pay and allowances as authorized by the President.

Executive Order 12356—National security information

SOURCE: The provisions of Executive Order 12356 of Apr. 2, 1982, appear at 47 FR 14874 and 15557, 3 CFR, 1982 Comp., p. 166, unless otherwise noted.

TABLE OF CONTENTS

PREAMBLE

PART 1. *Original Classification*

1.1 Classification Levels..... [651]

Chapter 32—National Defense

1.2 Classification Authority.....	[652]
1.3 Classification Categories.....	[654]
1.4 Duration of Classification.....	[655]
1.5 Identification and Markings.....	[655]
1.6 Limitations on Classification.....	[655]

PART 2. *Derivative Classification*

2.1 Use of Derivative Classification.....	[656]
2.2 Classification Guides.....	[656]

PART 3. *Declassification and Downgrading*

3.1 Declassification Authority.....	[657]
3.2 Transferred Information.....	[657]
3.3 Systematic Review for Declassification.....	[657]
3.4 Mandatory Review for Declassification.....	[658]

PART 4. *Safeguarding*

4.1 General Restrictions on Access.....	[659]
4.2 Special Access Programs.....	[659]
4.3 Access by Historical Researchers and Former Presidential Appointees.....	[660]

PART 5. *Implementation and Review*

5.1 Policy Direction.....	[660]
5.2 Information Security Oversight Office.....	[660]
5.3 General Responsibilities.....	[661]
5.4 Sanctions.....	[662]

PART 6. *General Provisions*

6.1 Definitions.....	[662]
6.2 General.....	[663]

This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security.

NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

PART 1

Original Classification

SECTION 1.1 *Classification Levels*

(a) National security information (hereinafter "classified information") shall be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information.

(c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

SEC. 1.2 Classification Authority.¹

¹ EDITORIAL NOTE: On May 7, 1982, the President issued an order of designation (47 FR 20105, 3 CFR, 1982 Comp., p. 257) the text of which follows:

Pursuant to the provisions of Section 1.2 of Executive Order No. 12356 of April 2, 1982, entitled "National Security Information," I hereby designate the following officials to classify information originally as "Top Secret", "Secret", or "Confidential":

TOP SECRET

Executive Office of the President:

The Vice President
The Counsellor to the President
The Chief of Staff and Assistant to the President
The Deputy Chief of Staff and Assistant to the President
The Director, Office of Management and Budget
The United States Trade Representative
The Assistant to the President for National Security Affairs
The Director, Office of Science and Technology Policy
The Chairman, The President's Foreign Intelligence Advisory Board
The Chairman, The President's Intelligence Oversight Board

The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
The Secretary of the Army
The Secretary of the Navy
The Secretary of the Air Force
The Attorney General
The Secretary of Energy
The Chairman, Nuclear Regulatory Commission
The Director, United States Arms Control and Disarmament Agency
The Director of Central Intelligence
The Administrator, National Aeronautics and Space Administration
The Administrator of General Services
The Director, Federal Emergency Management Agency

SECRET

Executive Office of the President:

The Chairman, Council of Economic Advisers
The President's Personal Representative for Micronesian Status Negotiations
The Secretary of Commerce
The Secretary of Transportation
The Administrator, Agency for International Development
The Director, International Communication Agency

(a) *Top Secret*. The authority to classify information originally as Top Secret may be exercised only by:

- (1) the President;
- (2) agency heads and officials designated by the President in the FEDERAL REGISTER; and
- (3) officials delegated this authority pursuant to Section 1.2(d).

(b) *Secret*. The authority to classify information originally as Secret may be exercised only by:

- (1) agency heads and officials designated by the President in the FEDERAL REGISTER;
- (2) officials with original Top Secret classification authority; and
- (3) officials delegated such authority pursuant to Section 1.2(d).

(c) *Confidential*. The authority to classify information originally as Confidential may be exercised only by:

- (1) agency heads and officials designated by the President in the FEDERAL REGISTER;
- (2) officials with original Top Secret or Secret classification authority; and
- (3) officials delegated such authority pursuant to Section 1.2(d).

(d) *Delegation of Original Classification Authority*.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a)(1),¹ provided that official has been delegated original Top Secret classification authority by the agency head.

(3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1),¹ provided that official has been delegated original Secret classification authority by the agency head.

(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1),¹ provided that official has been delegated original classification authority by the agency head.

CONFIDENTIAL

The President, Export-Import Bank of the United States
The President, Overseas Private Investment Corporation
The Administrator, Environmental Protection Agency

Any delegation of this authority shall be in accordance with Section 1.2(d) of the Order.

This Order shall be published in the FEDERAL REGISTER.

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

(5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.

(e) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

SEC. 1.3 *Classification Categories.*

- (a) Information shall be considered for classification if it concerns:
- (1) military plans, weapons, or operations;
 - (2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
 - (3) foreign government information;
 - (4) intelligence activities (including special activities), or intelligence sources or methods;
 - (5) foreign relations or foreign activities of the United States;
 - (6) scientific, technological, or economic matters relating to the national security;
 - (7) United States Government programs for safeguarding nuclear materials or facilities;
 - (8) cryptology;
 - (9) a confidential source; or
 - (10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.
- (b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.
- (c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.
- (d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or in-

advertent or unauthorized disclosure in the United States or abroad of identical or similar information.

SEC. 1.4 *Duration of Classification.*

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

SEC. 1.5 *Identification and Markings.*

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

- (1) one of the three classification levels defined in Section 1.1;
- (2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;
- (3) the agency and office of origin; and
- (4) the date or event for declassification, or the notation "Originating Agency's Determination Required."

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).

SEC. 1.6 *Limitations on Classification.*

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to

prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1),¹ or an official with original Top Secret classification authority.

PART 2

Derivative Classification

SEC. 2.1 Use of Derivative Classification.

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

SEC. 2.2 Classification Guides.

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official designated under Section 5.3(a)(1);¹ and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

(c) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

PART 3

Declassification and Downgrading

SEC. 3.1 Declassification Authority.

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order.

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1).¹

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal.

(d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but that had such authority under predecessor orders.

SEC. 3.2 Transferred Information.

(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

(b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.

SEC. 3.3 Systematic Review for Declassification.

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

(a) The Archivist of the United States shall, in accordance with procedures and timeframes prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivist's control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.

(b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

SEC. 3.4 *Mandatory Review for Declassification.*

(a) Except as provided in Section 3.4(b), all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if:

- (1) the request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and
- (2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order.

They shall release this information unless withholding is otherwise authorized under applicable law.

(d) Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request.

(e) The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

(f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:

(1) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.

PART 4

Safeguarding

SEC. 4.1 *General Restrictions on Access.*

(a) 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.

(b) Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

(c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.

(d) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

SEC. 4.2 *Special Access Programs.*

(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence.

(b) Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non-delegable access to all such accountings.

SEC. 4.3 Access by Historical Researchers and Former Presidential Appointees.

(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who:

- (1) are engaged in historical research projects, or
- (2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under Section 4.3(a) may be granted only if the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and

(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

PART 5

Implementation and Review

SEC. 5.1 Policy Direction.

(a) The National Security Council shall provide overall policy direction for the information security program.

(b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

SEC. 5.2 Information Security Oversight Office.

(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.

(b) The Director shall:

(1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order, which shall be binding on the agencies;

(2) oversee agency actions to ensure compliance with this Order and implementing directives;

(3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a)(1)¹ may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program;

(7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program;

(8) report at least annually to the President through the National Security Council on the implementation of this Order; and

(9) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

SEC. 5.3 General Responsibilities.

Agencies that originate or handle classified information shall:

(a) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;

(b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the FEDERAL REGISTER to the extent that these regulations affect members of the public;

(c) establish procedures to prevent unnecessary access to classified information, including procedures that (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified information is limited to the mini-

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

and
mum consistent with operational and security requirements and

(d) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.

SEC. 5.4 Sanctions.

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency to the senior official designated under Section 5.3(a)(1) ¹ so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and contractors, licensees, and grantees shall be subject to appropriate sanctions if they:

(1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders;

(2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive;

(3) knowingly and willfully violate any other provision of this Order or implementing directive.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) Each agency head or the senior official designated under Section 5.3(a)(1) ¹ shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b) (1) or (2) occurs.

PART 6

General Provisions

SEC. 6.1 Definitions.

(a) "Agency" has the meaning provided at 5 U.S.C. 552(e).

(b) "Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(d) "Foreign government information" means:

(1) information provided by a foreign government or government, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or govern-

¹ EDITORIAL NOTE: The correct citation is Section 5.3(a).

ments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(e) "National security" means the national defense or foreign relations of the United States.

(f) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

SEC. 6.2 General.

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

(c) Nothing in this Order limits the protection afforded any information by other provisions of law.

(d) Executive Order No. 12065 of June 28, 1978, as amended, is revoked as of the effective date of this Order.

(e) This Order shall become effective on August 1, 1982.

Executive Order 12537—President's Foreign Intelligence Advisory Board

SOURCE: The provisions of Executive Order 12537 of Oct. 28, 1985, appear at 50 FR 45083, 3 CFR, 1985 Comp., p. 394, unless otherwise noted.

By the authority vested in me as President by the Constitution and statutes of the United States of America, and in order to enhance the security of the United States by improving the quality and effectiveness of intelligence available to the United States, it is ordered as follows:

SECTION 1. There is hereby established within the White House Office, Executive Office of the President, the President's Foreign Intelligence Advisory Board (the "Board"). The Board shall consist of not more than sixteen members, who shall serve at the pleasure of the President and shall be appointed by the President from among trustworthy and distinguished citizens outside the government who are qualified on the basis of achievement, experience, and independence. The President shall establish the terms of the members upon their appointment. To the extent practicable, one-third of the Board at any one time shall be comprised of members whose current term of service does not exceed two years. The President shall designate a Chairman and Vice Chairman from among the members. The Board shall utilize full-

designations per F.O. 12356

Other Presidential Documents

Presidential Determination No. 90-20 of May 19, 1990

Determination To Authorize Assistance through the Organization of American States for Nicaragua

Memorandum for the Secretary of State

By virtue of the authority vested in me by Section 451 of the Foreign Assistance Act of 1961, as amended, 22 U.S.C. 2261, I hereby authorize the use of up to \$1.25 million in funds to be made available under Chapter 3 of Part I of the Act in Fiscal Year 1990 for emergency assistance through the Organization of American States to Nicaragua notwithstanding any other provision of law. The assistance is provided in order to care for and feed members of the Nicaraguan Resistance who are located in designated security zones under appropriate agreements with the Government of Nicaragua for their demobilization and resettlement.

You are authorized and directed to report this determination to the Speaker of the House of Representatives, the House Appropriations Committee, and the Senate Committees on Foreign Relations and Appropriations immediately, and to publish it in the Federal Register.

GEORGE BUSH

THE WHITE HOUSE,
Washington, May 19, 1990.

Presidential Determination No. 90-21 of May 24, 1990

Determination Under Subsection 402(d)(5) of the Trade Act of 1974—Continuation of Waiver Authority

Memorandum for the Secretary of State

Pursuant to the authority vested in me under the Trade Act of 1974 (Public Law 93-618), January 3, 1975 (88 Stat. 1978) (hereinafter "the Act"), I determine, pursuant to subsection 402(d)(5) of the Act, 19 U.S.C. 2432(d)(5), that the further extension of the waiver authority granted by subsection 402(c) of the Act will substantially promote the objectives of section 402 of the Act. I further determine that the continuation of the waiver applicable to the People's Republic of China will substantially promote the objectives of section 402 of the Act.

You are authorized and directed to publish this determination in the Federal Register.

GEORGE BUSH

THE WHITE HOUSE,
Washington, May 24, 1990.

Editorial note: For the President's message to the Congress and the statement by Press Secretary Fitzwater on the renewal of the most-favored-nation trade status for China, see the *Weekly Compilation of Presidential Documents* (vol. 26, p. 827). For a statement issued by the President on

Memorandum for the Secretary of State

Pursuant to Section 2(c)(1) of the Migration and Refugee Assistance Act of 1962, as amended, 22 U.S.C. 2601(c)(1), I hereby determine that it is important to the national interest that \$7,000,000 be made available from the Emergency Refugee and Migration Assistance Fund (Emergency Fund) to meet unexpected urgent needs of Palestinian refugees. This \$7,000,000 would be contributed to the UN Relief and Works Agency for Palestine Refugees in the Near East (UNRWA) for its programs of relief, education and health care for Palestinian refugees. Without the \$7,000,000, UNRWA would be forced to cut essential services to the refugees.

You are authorized and directed to inform the Speaker of the House of Representatives and the appropriate committees of the Congress of this Determination and the obligation of funds under this authority, and to publish it in the Federal Register.

GEORGE BUSH

THE WHITE HOUSE,
Washington, April 28, 1990.

Order of May 4, 1990

✓ Pursuant to the provisions of Section 1.2 of Executive Order No. 12356 of April 2, 1982, entitled "National Security Information," I hereby designate the Director of National Drug Control Policy to classify information originally as "Top Secret."

This order shall be published in the Federal Register.

GEORGE BUSH

THE WHITE HOUSE,
May 4, 1990.

**PART 2000—ADMINISTRATIVE
PROCEDURES [RESERVED]**

**PART 2001—NATIONAL SECURITY
INFORMATION**

Subpart A—Original Classification

Sec.

- 2001.1 Classification levels.
- 2001.2 Classification authority.
- 2001.3 Classification categories.
- 2001.4 Duration of classification.
- 2001.5 Identification and markings [1.5(a), 1.5(b) and 1.5(c)].
- 2001.6 Limitations on classification [1.6(c)].

Subpart B—Derivative Classification

- 2001.20 Use of derivative classification [2.1].
- 2001.21 Classification guides.
- 2001.22 Derivative identification and markings [1.5(c) and 2.1(b)].

Subpart C—Declassification and Downgrading

- 2001.30 Listing declassification and downgrading authorities [3.1(b)].
- 2001.31 Systematic review for declassification [3.3].
- 2001.32 Mandatory review for declassification [3.4].
- 2001.33 Assistance to the Department of State [3.3(b)].
- 2001.34 FOIA and Privacy Act requests [3.4].

Subpart D—Safeguarding

- 2001.40 General [4.1].
- 2001.41 Standards for security equipment [4.1(b) and 5.1(b)].
- 2001.42 Accountability [4.1(b)].
- 2001.43 Storage [4.1(b)].
- 2001.44 Transmittal [4.1(b)].
- 2001.45 Special access programs [1.2(a) and 4.2(a)].
- 2001.46 Reproduction controls [4.1(b)].
- 2001.47 Loss or possible compromise [4.1(b)].
- 2001.48 Disposition and destruction [4.1(b)].
- 2001.49 Responsibilities of holders [4.1(b)].
- 2001.50 Emergency planning [4.1(b)].
- 2001.51 Emergency authority [4.1(b)].

Subpart E—Implementation and Review

- 2001.60 Agency regulations [5.3(b)].
- 2001.61 Security education [5.3(a)].
- 2001.62 Oversight [5.3(a)].

Sec.

Subpart F—General Provisions

- 2001.70 Definitions [6.1].
- 2001.71 Publication and effective date [6.2(e)].

AUTHORITY: Sec. 5.2(b)(1), E.O. 12356, 47 FR 14874, April 6, 1982.

SOURCE: Directive No. 1, 47 FR 27836, June 25, 1982, unless otherwise noted.

Subpart A—Original Classification

§ 2001.1 Classification levels.

(a) *Limitations [1.1(b)].* Markings other than "Top Secret," "Secret," and "Confidential," such as "For Official Use Only" or "Limited Official Use," shall not be used to identify national security information. No other term or phrase shall be used in conjunction with these markings, such as "Secret Sensitive" or "Agency Confidential," to identify national security information. The terms "Top Secret," "Secret," and "Confidential" should not be used to identify nonclassified executive branch information.

(b) *Reasonable doubt [1.1(c)].* (1) When there is reasonable doubt about the need to classify information, the information shall be safeguarded as if it were "Confidential" information in accordance with subpart D, pending the determination about its classification. Upon the determination of a need for classification, the information that is classified shall be marked as provided in § 2001.5.

(2) When there is reasonable doubt about the appropriate classification level, the information shall be safeguarded at the higher level in accordance with subpart D, pending the determination about its classification level. Upon the determination of its classification level, the information shall be marked as provided in § 2001.5.

§ 2001.2 Classification authority.

(a) *Requests for original classification authority [1.2 and 5.2(b)(5)].* A request for original classification authority pursuant to section 1.2 of Ex-

¹ Bracketed references pertain to related sections of Executive Order 12356.

Information Security Oversight Office

§ 2001.5

ecutive Order 12356 (hereinafter "the Order") shall include a complete justification for the level of classification authority sought, a description of the information that will require original classification, and the anticipated frequency of original classification actions.

(b) *Listing classification authorities [1.2].* Agencies shall maintain a current listing of officials delegated original classification authority by name, position, or other identifier. If possible, this listing shall be unclassified.

(c) *Exceptional cases [1.2(e)].* Information described in section 1.2(e) of the Order shall be protected as provided in § 2001.1(b).

§ 2001.3 Classification categories.

(a) *Classification in context of related information [1.3(b)].* Certain information which would otherwise be unclassified may require classification when combined or associated with other unclassified or classified information. Classification on this basis shall be supported by a written explanation that, at a minimum, shall be maintained with the file or referenced on the record copy of the information.

(b) *Unofficial publication or disclosure [1.3(d)].* Following an inadvertent or unauthorized publication or disclosure of information identical or similar to information that has been classified in accordance with the Order or predecessor orders, the agency of primary interest shall determine the degree of damage to the national security, the need for continued classification, and, in coordination with the agency in which the disclosure occurred, what action must be taken to prevent similar occurrences.

§ 2001.4 Duration of classification.

(a) *Information not marked for declassification [1.4].* Information classified under predecessor orders that is not subject to automatic declassification shall remain classified until reviewed for declassification.

(b) *Authority to extend automatic declassification determinations [1.4(b)].* The authority to extend the classification of information subject to automatic declassification under predecessor orders is limited to those offi-

cials who have classification authority over the information and are designated in writing to have original classification authority at the level of the information to remain classified. Any decision to extend this classification on other than a document-by-document basis shall be reported to the Director of the Information Security Oversight Office.

§ 2001.5 Identification and markings [1.5(a), 1.5(b) and 1.5(c)].

A uniform information security system requires that standard markings be applied to national security information. Except in extraordinary circumstances as provided in section 1.5(a) of the Order, or as indicated herein, the marking of paper documents created after the effective date of the Order shall not deviate from the following prescribed formats. These markings shall also be affixed to material other than paper documents, or the originator shall provide holders or recipients of the information with written instructions for protecting the information.

(a) *Classification level.* The markings "Top Secret," "Secret," and "Confidential" are used to indicate: that information requires protection as national security information under the Order; the highest level of classification contained in a document; and the classification level of each page and, in abbreviated form, each portion of a document.

(1) *Overall marking.* The highest level of classification of information in a document shall be marked in such a way as to distinguish it clearly from the informational text. These markings shall appear at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

(2) *Page marking.* Each interior page of a classified document shall be marked at the top and bottom either according to the highest classification of the content of the page, including the designation "Unclassified" when it is applicable, or with the highest overall classification of the document.

(3) *Portion marking.* Agency heads may waive the portion marking requirement for specified classes of documents or information only upon a written determination that:

(i) There will be minimal circulation of the specified documents or information and minimal potential usage of these documents or information as a source for derivative classification determinations; or (ii) there is some other basis to conclude that the potential benefits of portion marking are clearly outweighed by the increased administrative burdens. Unless the portion marking requirement has been waived as authorized, each portion of a document, including subjects and titles, shall be marked by placing a parenthetical designation immediately preceding or following the text to which it applies. The symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used for this purpose. If the application of parenthetical designations is not practicable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification, and the information that is not classified. If all portions of a document are classified at the same level, this fact may be indicated by a statement to that effect. If a subject or title requires classification, an unclassified identifier may be applied to facilitate reference.

(b) *Classification authority.* If the original classifier is other than the signer or approver of the document, the identity shall be shown as follows:

CLASSIFIED BY (identification of original classification authority)

(c) *Agency and office of origin.* If the identity of the originating agency and office is not apparent on the face of a document, it shall be placed below the "CLASSIFIED BY" line.

(d) *Declassification and downgrading instructions.* Declassification and, as applicable, downgrading instructions shall be shown as follows:

(1) For information to be declassified automatically on a specific date:

DECLASSIFY ON: (date)

(2) For information to be declassified automatically upon occurrence of a specific event:

DECLASSIFY ON: (description of event)

(3) For information not to be declassified automatically:

DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED or "OADR"

(4) For information to be downgraded automatically on a specific date or upon occurrence of a specific event:

DOWNGRADE TO (classification level) **ON** (date or description of event)

(e) *Special markings—(1) Transmittal documents [1.5(c)].* A transmittal document shall indicate on its face the highest classification of any information transmitted by it. It shall also include the following or similar instruction:

(i) For an unclassified transmittal document:

UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE IS REMOVED

(ii) For a classified transmittal document:

UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS (classification level of the transmittal document standing alone)

(2) *"Restricted Data" and "Formerly Restricted Data" [6.2(a)].* "Restricted Data" and "Formerly Restricted Data" shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended.

(3) *Intelligence sources or methods [1.5(c)].* Documents that contain information relating to intelligence sources or methods shall include the following marking unless otherwise proscribed by the Director of Central Intelligence:

WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED

(4) *Foreign government information [1.5(c)].* Documents that contain foreign government information shall include either the marking "FOREIGN GOVERNMENT INFORMATION," or a marking that otherwise indicates that the information is foreign government information. If the fact that in-

formation is foreign government information must be concealed, the marking shall not be used and the document shall be marked as if it were wholly of U.S. origin.

(5) *Computer output [1.5(c)].* Documents that are generated as computer output may be marked automatically by systems software. If automatic marking is not practicable, such documents must be marked manually.

(6) *Agency prescribed markings [1.5(c), 4.2(a), and 5.3(c)].* Officials delegated original classification authority by the President may prescribe additional markings to control reproduction and dissemination, including markings required for special access programs authorized by section 4.2(a) of the Order.

(f) *Electrically transmitted information (messages) [1.5(c)].* National security information that is transmitted electrically shall be marked as follows:

(1) The highest level of classification shall appear before the first line of text;

(2) A "CLASSIFIED BY" line is not required;

(3) The duration of classification shall appear as follows:

(i) For information to be declassified automatically on a specific date:

DECL: (date)

(ii) For information to be declassified upon occurrence of a specific event:

DECL: (description of event)

(iii) For information not to be automatically declassified which requires the originating agency's determination (see also § 2001.5(d)(3)):

DECL: OADR

(iv) For information to be automatically downgraded:

DNG (abbreviation of classification level to which the information is to be downgraded and date or description of event on which downgrading is to occur)

(4) Portion marking shall be as prescribed in § 2001.5(a)(3);

(5) Special markings as prescribed in § 2001.5(e) (2), (3), and (4) shall appear after the marking for the highest level of classification. These include:

(i) "Restricted Data" and "Formerly Restricted Data" shall be marked in accordance with regulations issued under the Atomic Energy Act of 1954, as amended;

(ii) Information concerning intelligence sources or methods: "WNINTEL," unless proscribed by the Director of Central Intelligence;

(iii) Foreign government information: "FGI," or a marking that otherwise indicates that the information is foreign government information. If the fact that information is foreign government information must be concealed, the marking shall not be used and the message shall be marked as if it were wholly of U.S. origin.

(6) Paper copies of electrically transmitted messages shall be marked as provided in § 2001.5(a) (1) and (2).

(g) *Changes in classification markings [1.4(b) and 4.1(b)].* When a change is made in the duration of classified information, all holders of record shall be promptly notified. If practicable, holders of record shall also be notified of a change in the level of classification. Holders shall alter the markings to conform to the change, citing the authority for it. If the remarking of large quantities of information is unduly burdensome, the holder may attach a change of classification notice to the storage unit in lieu of the marking action otherwise required. Items withdrawn from the collection for purposes other than transfer for storage shall be marked promptly in accordance with the change notice.

§ 2001.6 Limitations on classification [1.6(c)].

Before reclassifying information as provided in section 1.6(c) of the Order, the authorized official shall consider the following factors, which shall be addressed in the report to the Director of the Information Security Oversight Office:

(a) The elapsed time following disclosure;

(b) The nature and extent of disclosure;

(c) The ability to bring the fact of reclassification to the attention of per-

sons to whom the information was disclosed;

(d) The ability to prevent further disclosure; and

(e) The ability to retrieve the information voluntarily from persons not authorized access in its reclassified state.

Subpart B—Derivative Classification

§ 2001.20 Use of derivative classification [2.1].

The application of derivative classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form information that is already classified, and of those who apply markings in accordance with instructions from an authorized original classifier or in accordance with an authorized classification guide. If a person who applies derivative classification markings believes that the paraphrasing, restating, or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult for a determination an appropriate official of the originating agency or office of origin who has the authority to upgrade, downgrade, or declassify the information.

§ 2001.21 Classification guides.

(a) *General* [2.2(a)]. Classification guides shall, at a minimum:

(1) Identify or categorize the elements of information to be protected;

(2) State which classification level applies to each element or category of information; and

(3) Prescribe declassification instructions for each element or category of information in terms of (i) a period of time, (ii) the occurrence of an event, or (iii) a notation that the information shall not be declassified automatically without the approval of the originating agency.

(b) *Requirement for review* [2.2(a)]. Classification guides shall be reviewed at least every two years and updated as necessary. Each agency shall maintain a list of its classification guides in current use.

(c) *Waivers* [2.2(c)]. An authorized official's decision to waive the requirement to issue classification guides for

specific classes of documents or information should be based, at a minimum, on an evaluation of the following factors:

(1) The ability to segregate and describe the elements of information;

(2) The practicality of producing or disseminating the guide because of the nature of the information;

(3) The anticipated usage of the guide as a basis for derivative classification; and

(4) The availability of alternative sources for derivatively classifying the information in a uniform manner.

§ 2001.22 Derivative identification and markings [1.5(c) and 2.1(b)].

Documents classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in § 2001.5(a) through (e) as are applicable. Information for these markings shall be taken from the source document or instructions in the appropriate classification guide.

(a) *Classification authority*. The authority for classification shall be shown as follows:

CLASSIFIED BY (description of source document or classification guide)

If a document is classified on the basis of more than one source document or classification guide, the authority for classification shall be shown as follows:

CLASSIFIED BY MULTIPLE SOURCES

In these cases the derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. A document derivatively classified on the basis of a source document that is marked "CLASSIFIED BY MULTIPLE SOURCES" shall cite the source document in its "CLASSIFIED BY" line rather than the term "MULTIPLE SOURCES."

(b) *Declassification and downgrading instructions*. Dates or events for automatic declassification or downgrading, or the notation "ORIGINATING AGENCY'S DETERMINATION REQUIRED" to indicate that the document is not to be declassified automatically, shall be carried forward from the source document, or as di-

rected by a classification guide, and shown on a "DECLASSIFY ON" line as follows:

DECLASSIFY ON: (date; description of event; or "ORIGINATING AGENCY'S DETERMINATION REQUIRED" (OADR))

Subpart C—Declassification and Downgrading

§ 2001.30 Listing declassification and downgrading authorities [3.1(b)].

Agencies shall maintain a current listing of officials delegated declassification or downgrading authority by name, position, or other identifier. If possible, this listing shall be unclassified.

§ 2001.31 Systematic review for declassification [3.3].

(a) *Permanent records*. Systematic review is applicable only to those classified records and presidential papers or records that the Archivist of the United States, acting under the Federal Records Act, has determined to be of sufficient historical or other value to warrant permanent retention.

(b) *Non-permanent records*. Non-permanent classified records shall be disposed of in accordance with schedules approved by the Administrator of General Services under the Records Disposal Act. These schedules shall provide for the continued retention of records subject to an ongoing mandatory review for declassification request.

(c) *Responsibilities*. (1) In meeting responsibilities assigned by section 3.3(a) of the Order, the Archivist shall:

(i) Establish procedures, in consultation with the Director of the Information Security Oversight Office, for the systematic declassification review of permanent classified records accessioned into the National Archives and classified presidential papers or records under the Archivist's control;

(ii) Conduct systematic declassification reviews in accordance with guidelines provided by the head of the agency that originated the information; or, with respect to foreign government information, in accordance with guidelines provided by the head

of the agency having declassification jurisdiction over the information, or, if no guidelines have been provided, in accordance with the general guidelines provided by the Director of the Information Security Oversight Office after coordination with the agencies having declassification authority over the information; or, with respect to presidential papers or records, in accordance with guidelines developed by the Archivist and approved by the National Security Council;

(iii) Conduct systematic declassification reviews of accessioned records and presidential papers or records as they become 30 years old, except for file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945, and information concerning cryptology created after 1945;

(iv) Conduct systematic declassification reviews of accessioned records and presidential papers or records in file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945 and cryptology records created after 1945 as they become fifty years old;

(v) Establish systematic review priorities for accessioned records and presidential papers or records based on the degree of researcher interest and the potential for declassifying a significant portion of the information;

(vi) Re-review for declassification accessioned records and presidential papers or records upon the determination that the followup review will be productive, both in terms of researcher interest and the potential for declassifying a significant portion of the information.

(2) The Archivist may review for declassification, with the concurrence of the originating agency, accessioned records and presidential papers or records, prior to the timeframes established in paragraphs (c)(1) (iii) and (iv) of this section.

(3) Officials delegated original classification authority by the President under the Order or predecessor orders shall:

(i) Within six months of the effective date of the Order issue guidelines for systematic declassification review

and, if applicable, for downgrading. These guidelines shall be developed in consultation with the Archivist and the Director of the Information Security Oversight Office and be designed to assist the Archivist in the conduct of systematic reviews;

(ii) Designate experienced personnel to provide timely assistance to the Archivist in the systematic review process;

(iii) Review and update guidelines for systematic declassification review and downgrading at least every five years unless earlier review is requested by the Archivist.

(4) Within six months of the effective date of the Order the Director of the Information Security Oversight Office shall issue, in consultation with the Archivist and the agencies having declassification authority over the information, general guidelines for the systematic declassification review of foreign government information. Also within six months, agency heads may issue, in consultation with the Archivist and the Director of the Information Security Oversight Office, specific systematic declassification review guidelines for foreign government information over which the agency head has declassification authority. These guidelines shall be reviewed and updated every five years unless earlier review is requested by the Archivist.

(d) *Special procedures.* All agency heads shall be bound by the special procedures for systematic review of classified cryptologic records and classified records pertaining to intelligence activities (including special activities), or intelligence sources or methods issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

§ 2001.32 Mandatory review for declassification [3.4].

(a) *U.S. originated information.* (1) Each agency head shall publish in the *FEDERAL REGISTER* the identity of the person(s) or office(s) to which mandatory declassification review requests may be addressed.

(2) *Processing—(i) Requests for classified records in the custody of the originating agency.* A valid mandatory declassification review request need

not identify the requested information by date or title of the responsive records, but must be of sufficient particularity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. Agency responses to mandatory declassification review requests shall be governed by the amount of search and review time required to process the request. In responding to mandatory declassification review requests, agencies shall either make a prompt declassification determination and notify the requester accordingly, or inform the requester of the additional time needed to process the request. Agencies shall make a final determination within one year from the date of receipt except in unusual circumstances. When information cannot be declassified in its entirety, agencies will make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Upon the denial of an initial request, the agency shall also notify the requester of the right of an administrative appeal, which must be filed within 60 days of receipt of the denial.

(ii) *Requests for classified records in the custody of an agency other than the originating agency.* When an agency receives a mandatory declassification review request for records in its possession that were originated by another agency, it shall forward the request to that agency. The forwarding agency shall include a copy of the records requested together with its recommendations for action. Upon receipt, the originating agency shall process the request in accordance with § 2001.32(a)(2)(i). Upon request, the originating agency shall communicate its declassification determination to the referring agency.

(iii) *Appeals of denials of mandatory declassification review requests.* The agency appellate authority shall normally make a determination within 30 working days following the receipt of an appeal. If additional time is required to make a determination, the agency appellate authority shall notify the requester of the additional time needed and provide the requester

with the reason for the extension. The agency appellate authority shall notify the requester in writing of the final determination and of the reasons for any denial.

(b) *Foreign government information.* Except as provided in this paragraph, agency heads shall process mandatory declassification review requests for classified records containing foreign government information in accordance with § 2001.32(a). The agency that initially received or classified the foreign government information shall be responsible for making a declassification determination after consultation with concerned agencies. If the agency receiving the request is not the agency that received or classified the foreign government information, it shall refer the request to the appropriate agency for action. Consultation with the foreign originator through appropriate channels may be necessary prior to final action on the request.

(c) *Cryptologic and intelligence information.* Mandatory declassification review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in accordance with special procedures issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

(d) *Fees.* In responding to mandatory declassification review requests for classified records, agency heads may charge fees in accordance with section 483a of title 31, United States Code. The schedules of fees published in the *FEDERAL REGISTER* by agencies in implementation of Executive Order 12065 shall remain in effect until they are revised.

§ 2001.33 Assistance to the Department of State [3.3(b)].

Heads of agencies should assist the Department of State in its preparation of the *Foreign Relations of the United States* (FRUS) series by facilitating access to appropriate classified material in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

§ 2001.34 FOIA and Privacy Act requests [3.4].

Agency heads shall process requests for declassification that are submitted under the provisions of the Freedom of Information Act, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

Subpart D—Safeguarding

§ 2001.40 General [4.1].

Information classified pursuant to this Order or predecessor orders shall be afforded a level of protection against unauthorized disclosure commensurate with its level of classification. For information in special access programs established under the provisions of section 4.2 of the Order, the safeguarding requirements of subpart D may be modified by the agency head responsible for creating the special access program as long as the modified requirements provide appropriate protection for the information.

§ 2001.41 Standards for security equipment [4.1(b) and 5.1(b)].

The Administrator of General Services shall, in coordination with agencies originating classified information, establish and publish uniform standards, specifications, and supply schedules for security equipment designed to provide secure storage for and to destroy classified information. Any agency may establish more stringent standards for its own use. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above and shall, to the maximum extent practicable, be of the type available through the Federal Supply System.

§ 2001.42 Accountability [4.1(b)].

(a) *Top Secret.* Top Secret control officials shall be designated to receive, transmit, and maintain current access and accountability records for Top Secret information. An inventory of Top Secret documents shall be made at least annually. Agency heads may waive the requirement for an annual inventory of storage systems containing large volumes of Top Secret information.

mation upon a determination that the safeguarding of this information is not jeopardized by the inventory waiver. Waivers shall be in writing and be available for review by the Information Security Oversight Office.

(b) *Secret and Confidential.* Agency heads shall prescribe accountability or control requirements for Secret and Confidential information.

§ 2001.43 Storage [4.1(b)].

Classified information shall be stored only in facilities or under conditions designed to prevent unauthorized persons from gaining access to it.

(a) *Minimum requirements for physical barriers—(1) Top Secret.* Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type changeable combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet the standards for Top Secret established under the provisions of § 2001.41. For Top Secret information stored outside the United States, one or more of the following supplementary controls is required:

(i) The area that houses the security container or vault shall be subject to the continuous protection of guard or duty personnel;

(ii) Guard or duty personnel shall inspect the security container or vault at least once every two hours; or

(iii) The security container or vault shall be controlled by an alarm system to which a force will respond in person within 15 minutes.

In addition, heads of agencies shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored both within and outside the United States.

(2) *Secret and Confidential.* Secret and Confidential information shall be stored in a manner and under the conditions prescribed for Top Secret information, or in a container, vault, or alarmed area that meets the standards for Secret or Confidential information established under the provisions of § 2001.41. Secret and Confidential information may also be stored in a safe-type filing cabinet having a built-in,

three-position, dial-type changeable combination lock, or a steel filing cabinet equipped with a steel lock bar secured by a GSA-approved three-position changeable combination padlock. Heads of agencies shall prescribe supplementary controls for storage of Secret information in cabinets equipped with a steel lock bar. Access to bulky Secret and Confidential material in weapons storage areas, strong rooms, closed areas or similar facilities shall be controlled in accordance with requirements established by the appropriate agency head. At a minimum, such requirements shall prescribe the use of key-operated, high-security padlocks approved by the General Services Administration.

(b) *Combinations.* (1) *Equipment in service.* Combinations to dial-type locks shall be changed only by persons having an appropriate security clearance, and shall be changed whenever such equipment is placed in use; whenever a person knowing the combination no longer requires access to it; whenever a combination has been subjected to possible compromise; whenever the equipment is taken out of service; or at least once every year. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes. Records of combinations shall be classified no lower than the highest level of classified information that is protected by the lock.

(2) *Equipment out of service.* When security equipment is taken out of service it shall be inspected to ensure that no classified information remains, and the built-in combination lock shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30.

(c) *Keys.* Heads of agencies shall establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys shall be equivalent to that afforded the classified information being protected by the padlock.

(Directive No. 1, 47 FR 27836, June 25, 1982, as amended at 52 FR 28418, July 29, 1987)

§ 2001.44 Transmittal [4.1(b)].

(a) *Preparation and receipting.* Classified information to be transmitted outside of a facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that Confidential information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, the addressee, and the document, but shall contain no classified information. It shall be immediately signed by the recipient and returned to the sender. Any of these wrapping and receipting requirements may be waived by agency heads if conditions provide at least equivalent protection to prevent access by unauthorized persons.

(b) *Transmittal of Top Secret.* The transmittal of Top Secret information outside of a facility shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system authorized for the purpose, or over authorized secure communications circuits.

(c) *Transmittal of Secret.* The transmittal of Secret information shall be effected in the following manner:

(1) The 50 States, the District of Columbia, and Puerto Rico. Under such conditions as may be prescribed by the head of the agency concerned, Secret information may be transmitted within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico by one of the means authorized for Top Secret information; by the United States Postal Service registered mail or express mail service; or by protective services provided by United States air or surface commercial carriers. United States Postal Service express mail service shall be used only when it is the most effective means to accomplish a mission within security, time, cost, and accountability constraints. To ensure direct delivery to the addressee, the "Waiver of Signature and Indemnity" block on the United States

Postal Service Express Mail Label 11-B may not be executed under any circumstances. All Secret express mail shipments should be processed through mail distribution centers or delivered directly to a United States Postal Service facility or representative. The use of external (street side) express mail collection boxes is prohibited.

(2) *Other areas.* Secret information may be transmitted from, to, or within areas other than those specified in § 2001.44(c)(1) by one of the means established for Top Secret information, or by U.S. registered mail through Military Postal Service facilities provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system. Transmittal outside such areas may also be accomplished under escort of appropriately cleared personnel aboard U.S. Government and U.S. Government contract vehicles or aircraft, ships of the United States Navy, civil service manned U.S. Naval ships, and ships of U.S. registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are U.S. citizens and who are appropriately cleared may be designated as escorts.

(d) *Transmittal of Confidential.* Confidential information shall be transmitted within and between the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories or possessions by one of the means established for higher classifications, or by the U.S. Postal Service certified, first class, or express mail service when prescribed by an agency head. Outside these areas, Confidential information shall be transmitted only as is authorized for higher classifications.

(e) *Hand carrying of classified information.* Agency regulations shall prescribe procedures and appropriate restrictions concerning the escort or hand carrying of classified information, including the hand carrying of classified information on commercial carriers.

(Directive No. 1, 47 FR 27836, June 25, 1982, as amended at 55 FR 38030, Sept. 14, 1990)

§ 2001.45 Special access programs [1.2(a) and 1.2(a)].

Agency heads designated pursuant to section 1.2(a) of the Order may create or continue a special access program if:

(a) Normal management and safeguarding procedures do not limit access sufficiently; and

(b) The number of persons with access is limited to the minimum necessary to meet the objective of providing extra protection for the information.

§ 2001.46 Reproduction controls [1.1(b)].

(a) Top Secret documents, except for the controlled initial distribution of information processed or received electrically, shall not be reproduced without the consent of the originator.

(b) Unless restricted by the originating agency, Secret and Confidential documents may be reproduced to the extent required by operational needs.

(c) Reproduced copies of classified documents shall be subject to the same accountability and controls as the original documents.

(d) Paragraphs (a) and (b) of this section shall not restrict the reproduction of documents to facilitate review for declassification.

§ 2001.47 Loss or possible compromise [4.1(b)].

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated for this purpose by the person's agency or organization. The agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The following guidelines shall govern the conduct of damage assessments:

(a) *Initiation of Damage Assessments.* An agency head shall initiate a damage assessment whenever there has been a compromise of classified information originated by that agency that, in his or her judgment, can reasonably be expected to cause damage to the national security. Compromises

may occur through espionage, unauthorized disclosures to the press or other members of the public, unauthorized sales, publication of books and treatises, the known loss of classified information or equipment to foreign powers, or through various other circumstances.

(b) *Content of Damage Assessments.* At a minimum, damage assessments shall be in writing and contain the following:

(1) Identification of the source, date, and circumstances of the compromise.

(2) Classification of the specific information lost.

(3) A description of the specific information lost.

(4) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

(5) An assessment of the possible advantage to foreign powers resulting from the compromise.

(6) An assessment of whether (i) the classification of the information involved should be continued without change; (ii) the specific information, or parts thereof, shall be modified to minimize or nullify the effects of the reported compromise and the classification retained; (iii) downgrading, declassification, or upgrading is warranted, and if so, confirmation of prompt notification to holders of any change.

(7) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

(8) An assessment of other appropriate corrective, administrative, disciplinary or legal actions.

(c) *System of Control of Damage Assessments.* Each agency shall establish a system of control and internal procedures to ensure that damage assessments are performed in all cases described in paragraph (a), and that records are maintained in a manner that facilitates their retrieval and use within the agency.

(d) *Cases Involving More Than One Agency.* (1) Whenever a compromise involves the classified information or interests of more than one agency, each department or agency undertaking a damage assessment shall advise other agencies of the circumstances

and findings that affect their information or interests. Whenever a damage assessment, incorporating the product of two or more agencies is needed, the affected agencies shall agree upon the assignment of responsibility for the assessment.

(2) Whenever a compromise occurs within an agency that is not responsible for the damage assessment, that agency shall provide all data pertinent to the compromise to the agency responsible for conducting the assessment.

(3) Whenever a compromise of U.S. classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals in the employ of international organizations, the agency performing the damage assessment shall ensure through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one agency is responsible for the assessment, those agencies shall coordinate the request prior to transmittal through appropriate channels.

(4) Whenever an action is contemplated against any person believed responsible for the compromise of classified information, damage assessments shall be coordinated with appropriate agency legal counsel. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, the agency responsible for the damage assessment shall coordinate with the Department of Justice.

(5) The designated representative of the Director of Central Intelligence, or other appropriate officials with responsibility for the information involved, will be consulted whenever a compromise of Sensitive Compartmented Information (SCI) has occurred.

[49 FR 20789, May 16, 1984]

§ 2001.48 Disposition and destruction [4.1(b)].

Classified information no longer needed in current working files or for reference or record purposes shall be processed for appropriate disposition in accordance with the provisions of chapters 21 and 33 of title 44, United

States Code, which govern disposition of Federal records. Classified information approved for destruction shall be destroyed in accordance with procedures and methods prescribed by the head of the agency. The method of destruction must preclude recognition or reconstruction of the classified information or material.

§ 2001.49 Responsibilities of holders [4.1(b)].

Any person having access to and possession of classified information is responsible for: (a) Protecting it from persons not authorized access to it, to include securing it in approved equipment or facilities whenever it is not under the direct supervision of authorized persons; and (b) meeting accountability requirements prescribed by the head of the agency.

§ 2001.50 Emergency planning [4.1(b)].

Agencies shall develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, or enemy action. These plans shall include the disposition of classified information located in foreign countries.

§ 2001.51 Emergency authority [4.1(b)].

Those officials delegated original classification authority by the President may prescribe by regulation special provisions for the dissemination, transmittal, destruction, and safeguarding of national security information during combat or other emergency situations which pose an imminent threat to national security information.

Subpart E—Implementation and Review

§ 2001.60 Agency regulations [5.3(b)].

Each head of an agency shall issue regulations in accordance with 5 U.S.C. 552(a) to implement the Order and 32 CFR part 2001 no later than December 31, 1982. Those portions that affect members of the public shall include, at a minimum, information relating to the agency's mandatory declassification review program and instructions for submitting sugges-

tions or complaints regarding the agency's information security program.

§ 2001.61 Security education [5.3(a)].

Each agency that creates or handles national security information is required under the Order to establish a security education program. The program established shall be sufficient to familiarize all necessary personnel with the provisions of the Order and its implementing directives and regulations and to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

§ 2001.62 Overnight [5.3(a)].

Agency heads shall require that periodic formal reviews be made to ensure compliance with the provisions of the Order and ISOO directives.

Subpart F—General Provisions

§ 2001.70 Definitions [6.1].

(a) *Original classification authority.* The authority vested in an executive branch official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

(b) *Classification guide.* A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified on a derivative basis.

(c) *Originating agency.* The agency responsible for the initial determination that particular information is classified.

(d) *Multiple sources.* The term used to indicate that a document is derivatively classified when it contains classified information derived from more than one source.

(e) *Portion.* A segment of a document for purposes of expressing a unified theme; ordinarily a paragraph.

(f) *Special access program.* Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information.

Such a program may include, but is not limited to, special clearance, adjudication, or investigative requirements, special designations of officials authorized to determine "need-to-know," or special lists of persons determined to have a "need-to-know."

(g) *Intelligence activity.* An activity that an agency within the Intelligence Community is authorized to conduct pursuant to Executive Order 12333.

(h) *Special activity.* An activity conducted in support of national foreign policy objectives abroad which is planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activity, but which is not intended to influence United States political processes, public opinion, policies, or media and does not include diplomatic activities or the collection and production of intelligence or related support functions.

(i) *Unauthorized disclosure.* A communication or physical transfer of classified information to an unauthorized recipient.

§ 2001.71 Publication and effective date [6.2(e)].

Part 2001 shall be published in the FEDERAL REGISTER. It shall become effective August 1, 1982.

PART 2002—GENERAL GUIDELINES FOR SYSTEMATIC DECLASSIFICATION REVIEW OF FOREIGN GOVERNMENT INFORMATION

Sec.

2002.1 Purpose.

2002.2 Definition.

2002.3 Scope.

2002.4 Responsibilities.

2002.5 Effect of publication.

2002.6 Categories requiring item-by-item review.

2002.7 Referral and decision.

2002.8 Downgrading.

AUTHORITY: Sec. 3.3, E.O. 12356, 47 FR 14874, April 6, 1982.

SOURCE: 48 FR 4402, Jan. 31, 1983, unless otherwise noted.

§ 2002.1 Purpose.

These general guidelines for the systematic declassification review of for-

foreign government information have been developed in accordance with the provisions of section 3.3 of Executive Order 12356, "National Security Information," and § 2001.31 of Information Security Oversight Office Directive No. 1. All foreign government information that has been incorporated into the permanently valuable records of the United States Government and that has been accessioned into the National Archives of the United States shall be systematically reviewed for declassification by the Archivist of the United States. Declassification reviews shall be conducted in accordance with the provisions of these general guidelines or, if available, in accordance with specific systematic review guidelines for foreign government information provided by the agency heads who have declassification authority over that information. All foreign government information—

(a) Not identified in § 2002.6 of these general guidelines or in specific agency guidelines as requiring item-by-item declassification review and final determination by an agency declassification authority, and

(b) For which a prior declassification date has not been established, shall be declassified as that information becomes thirty years old.

§ 2002.2 Definition.

Foreign government information as used in these guidelines means:

(a) Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(b) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

§ 2002.3 Scope.

(a) These guidelines apply to foreign government information that has been

received or classified by the United States Government or its agents, and has been incorporated into records determined by the Archivist of the United States to have permanent value.

(b) Atomic energy information (including information originated prior to 1947 and not marked as such; information received from the United Kingdom or Canada marked "Atomic," or information received from NATO marked "Atomal") that is defined and identified as "Restricted Data" or "Formerly Restricted Data" in Sections 11y and 142d of the Atomic Energy Act of 1954, as amended, is outside the scope of these guidelines. Such information is not subject to systematic review and may not be automatically downgraded or declassified. Any document containing information within the definition of "Restricted Data" or "Formerly Restricted Data" that is not so marked shall be referred to the Department of Energy Office of Classification for review and appropriate marking, except for licensing and related regulatory matters which shall be referred to the Division of Security, U.S. Nuclear Regulatory Commission.

§ 2002.4 Responsibilities.

(a) Foreign government information transferred to the General Services Administration for accession into the National Archives of the United States shall be reviewed by the Archivist of the United States for declassification in accordance with Executive Order 12356, the directives of the Information Security Oversight Office, these general guidelines, and any specific systematic declassification guidelines provided by the agency with declassification authority over the information.

(b) Accessioned foreign government information in file series concerning intelligence activities (including special activities), or intelligence sources or methods created after 1945, and cryptology records created after 1945, shall be subject to review by the Archivist for declassification as it becomes 50 years old. All other accessioned foreign government information shall be subject to review by the

Cross-Cutting and Policy Issues

ISSUE: GAO Resumix Report

During the Transition, an evaluation of the existing Presidential Personnel Office (PPO) System was made to determine if it met the needs of the new Administration. The PPO system lacked sufficient flexibility and capacity. At that time, a number of systems were reviewed before the selection of Resumix. The systems reviewed included a custom designed system, Restrac (another commercial, off-the-shelf application), and Lotus Notes.

Resumix was chosen because it met the technical and operational requirements for the job. Resumix, along with a stand alone appointments tracking system, has replaced the system used by previous Administrations.

Resumix is a system of optical scanners, computer hardware, and software, that scan resumes and enable personnel staff to retrieve resumes by skill level, experience, interest and other variables.

Currently, there are 56,349 resumes in the system. There is a steadied usage for searches and retrievals on the seven terminals. The system will be upgraded in June 1994 at no additional cost. This upgrade was included in the purchase price of the system and will provide comment lines and document matching capabilities.

This system was originally leased for \$22,580 a month. It was purchased in August 1993 for \$225,800. To purchase the system, \$160,000 came from fiscal year 1993 WHO supplemental funding. It was determined that it was more cost effective to purchase the system than to continue with short term leases. If we had continued to lease at this rate, we would have paid as much for the system but would not have obtained ownership.

Based on inquiries from the Congressmen Jim Lightfoot, Frank Wolf and Ernest Istook, Jr., the General Accounting Office (GAO) conducted an audit on the acquisition of the Resumix system during June 1993. *In its report, GAO states that Resumix was an improvement over the existing PPO system - uses modern technology & less labor intensive. The report also noted that federal contracting regulations allow for sole-source contracting and since efforts were underway to meet the requirements; GAO did not make any negative recommendation. At present, the procurement file contains the justification and background requirements for the system.*

GAO did not report any evidence of problems with the operation of the Resumix system or financial ties to key White House personnel with the system's suppliers.

Finally, GAO did not make any adverse recommendations because the White House was adhering to federal contracting regulations.

As of March 3, 1994, GAO is conducting a follow-up review of the Resumix system to determine the final action taken since its report of June 1993.

Cross-Cutting and Policy Issues

ISSUE: GAO Personnel Report

Background

In April 1993, the General Accounting Office conducted an investigation into certain allegations concerning the backdating of White House appointments and salary adjustments. This investigation was performed at the request of Congressmen Lightfoot, Wolf and Istook.

The personnel actions in question, effective between January 20, 1993 and April 24, 1993, were made under one of two statutory employment authorizations.

Some personnel actions involved appointments or pay adjustments made under Title 5, U.S. Code, the personnel law that governs most appointments in the executive branch and contains specific requirements relating to the pay and position classification of employees.

A total of 611 appointments totaling \$335,787 and 69 salary increases or decreases totaling \$342,706 were examined. Most of the appointments and pay adjustments involved positions authorized under Title 3, U.S. Code.

While Title 3 contains certain limits on the number of appointments that are authorized at upper salary levels, it also stipulates that "The President is authorized to appoint and fix the pay of employees in the White House Office without regard to any other provision of law regulating the employment or compensation of persons in the Government service."

Retroactive Personnel Actions

GAO determined that 230 of the 611 appointments and 30 of the 69 salary adjustments were retroactive and involved individuals in a variety of Executive Office of the President offices and at varying salary levels. The retroactive payments involved were for modest amounts with the largest being \$3,720, while most others were less than \$400.

Although retroactive, these appointments and salary adjustments were legal. GAO has long held that a valid appointment is effective from the date the authorized appointing official approves the appointment and the employee performs work under supervision.

GAO concluded, based on the broad language of Title 3 and its legislative history, that such retroactive pay increases were proper.

There have been no retroactive appointments or pay adjustments since October 1, 1993.

Dual Payments and Other Personnel Matters

It was determined that 25 employees had overlapping salary periods from January 20, 1993 and February 20, 1993 totaling \$16,776. This total consisted of 10 employees repaying \$7,100 and the remaining 15 employees owing \$9,676..

This information was provided to the General Services Administration and White House officials for corrective actions.

As of March 14, 1994, a majority of the individuals had either paid their obligation in full. The remaining three individuals have made payment arrangements that were satisfactory to the General Services Administration (GSA).

New Procedures

We have revised the White House Personnel Manual which describes in plain English the procedures new employees should follow.

In addition, an experienced staff member within the Office of Administration has been assigned to the personnel management team responsible for the White House, the Office of the Vice President, and the Office of Policy Development to work with the agencies to ensure everything is being processed in a quick and efficient manner.

Also, there are biweekly meetings with administrative contacts from around the White House to discuss any problems which may occur.

TALKING POINTS ON THE WASHINGTON POST ARTICLE AND GAO AUDIT HEARINGS ARE ATTACHED.

original

THE WHITE HOUSE

WASHINGTON

June 15, 1994

Honorable Hank Brown
United States Senate
Washington, D.C. 20510-0604

Dear Senator Brown:

This is a response to your letter of March 22, 1994, requesting information about White House passes and other matters. Below please find answers to the specific questions you have raised.

1. Have any temporary passes been issued to personnel even though their Background Investigations have already been completed?

Yes. Before White House personnel may obtain permanent passes, they must satisfy numerous criteria including the satisfactory completion of the background investigation as well as a suitability review. This suitability review goes beyond that required for a security clearance and includes, among other items, a review of an employee's tax records, financial holdings, and memberships in social organizations. Portions of a suitability review may not have been completed at the time the background investigation has been favorably adjudicated. Thus, it is quite possible that personnel may hold temporary passes even though their FBI background investigations are complete.

2. Are personnel holding temporary passes receiving classified briefings, being allowed access to classified information, including the National Intelligence Daily (NID)?

As discussed above, a staff member may hold a temporary pass even though a background investigation has been adjudicated favorably, because other determinations have not been completed. In rare instances with a demonstrated need to know, Counsel's Office also may grant, on the basis of other available information, such as a prior background investigation, interim access to individuals whose background investigation is still pending. Thus, in some instances, White House personnel holding temporary passes have been cleared for national security purposes and have been allowed access to classified briefings or classified information. However, personnel who have not received appropriate security clearances may not have access to classified briefings or information.

In the White House, as in the rest of government, disclosure of classified information is provided strictly on a "need to know" basis. This principle is explicitly reaffirmed in the White House Staff Manual which states that, "Classified information may only be disclosed to persons who hold security clearances for the particular level of classification and have a need to know the information."

3. How many personnel continue to hold temporary passes, even though their Background Investigations have been completed?

As of the week of June 3, 1994, there were 38 Executive Office of the President (EOP) staff (including the White House Office, Office of Policy Development, Executive Residence, Office of the Vice President, the National Security Council and the Office of Administration as well as other offices but excluding the Office of Management and Budget and the United States Trade Representative), whose FBI background investigation is complete but whose file has not yet been forwarded to the Secret Service with a recommendation to issue a pass. All such individuals hold a temporary pass.

4. How many individuals have been issued permanent passes?

As of the week of June 3, 1994, 891 EOP personnel (as defined above) have been issued permanent passes.

5. What criteria constitute disqualification from receiving a permanent pass to the White House?

The White House adheres to the basic security criteria found in Executive Order 10450 and published in the Federal Personnel Manual (see attached). These criteria form the basis of judgments concerning permanent passes, and unfavorable evidence would provide the basis for any disqualification.

6. Have any temporary passes been issued for personnel assigned to work for the National Security Council (NSC), or who frequent work spaces occupied by the staff of the NSC?

Yes. As of May 23, there were 139 persons detailed to or employed by the National Security Council Staff. Of this number:

- 63 held Permanent White House passes (including one Other Government Agency pass);
- 45 held Temporary White House passes;
- 22 held Permanent EOB passes;
- 9 held Temporary EOB passes.

In addition, three contractors held Temporary White House passes in order to provide for training and maintenance on the NSC's computer system. Finally, and on occasion, anywhere from

two to ten executive branch employees may be assigned to work with the NSC staff on special projects, for example, to assist with document review and production in especially large cases.

All NSC employees (or persons utilizing NSC workspaces on an unrestricted basis) with permanent or temporary White House or Old Executive Office Building passes hold a top secret clearance with SCI access. NSC employees awaiting security clearances, persons pending assignment to the NSC staff, or any other government person who does not hold TS/SCI clearance, may not access the NSC computer system or enter secure areas unaccompanied. In addition, the White House Situation Room receives certification of clearances before permitting NSC employees access to national security information they have a need to know.

7. Have all personnel assigned to the NSC, or who frequent the work spaces occupied by the staff of the NSC, completed their background investigations?

Yes. All personnel assigned to the NSC staff who have access to classified information or work spaces containing classified information hold top secret clearances with SCI access.

Because the EOP requires a background investigation within one year of joining the staff of the EOP, for purposes of determining suitability to work at the White House, some NSC staff employees who already hold top secret clearances may undergo an updated background investigation in order to complete the suitability review and receive a permanent pass.

Sincerely,



Lloyd N. Cutler
Special Counsel to the President

Subchapter 5. Security Adjudication

5-1. BASIC SECURITY CRITERIA

Executive Order 10450 specifies security factors that should be considered when determining whether the employment, or retention in employment, of individuals in the Federal service is clearly consistent with the interests of the national security. The specified security criteria are:

- Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.
- Any deliberate misrepresentations, falsifications, or omission of material facts.
- Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.
- Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.
- Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause the person to act contrary to the best interests of the national security.
- Commission of any act of sabotage, espionage, treason, terrorism or sedition, or attempts thereat or preparation therefor, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, terrorism or sedition.
- Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist or revolutionist, or with an espionage or other secret agent or representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or the alteration of the form of government of the United States by unconstitutional means.
- Advocacy of use of force or violence to overthrow the Government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.
- Knowing membership, with specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons (hereinafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State, or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.
- Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.
- Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.
- Refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of alleged disloyalty or other misconduct.

NOTE: Because of Federal court decisions which have narrowed the grounds upon which an individual can be denied employment, the extent to which these factors can lead to disqualification is unclear.

WHITE HOUSE PRESS OFFICE



Facsimile Transmittal Sheet

To:

Chris Cerf

Fax Number:

57279

Office Number:

Comments:

WH passes fact sheet -

From the Office Of:

Fax Number:

Office Number:

FACT SHEET
WHITE HOUSE PASSES
Wednesday, March 23, 1994

Over the last several weeks, the White House has thoroughly reviewed the issuance of White House passes to tighten procedures.

Even before these steps were taken, existing practices and procedures ensured that White House personnel would not have access to the Complex until they had passed a preliminary security check. That check, which occurs before issuance of even a temporary pass, satisfies one of the principle objectives of a background investigation: minimizing the risk that dangerous or unstable individuals would have access to the White House Complex.

General Procedures

The White House and EOP follow a rigorous, multi-step process before issuing a permanent pass. Under current procedures, it takes, on average, four to five months to complete all phases of the process. The majority of that time (60 to 90 days) consists of a full field background check conducted by the FBI. In virtually every detail, the procedures followed by the Clinton Administration were and are consistent with those followed by previous administrations.

While these procedures are not new, it would be fair to say that the Administration has achieved greater operational efficiency over the last few months. As a result, the bottlenecks that previously delayed issuance of passes have been corrected, and we anticipate that the White House will be able to continue to process passes

... to continue to process passes in
approximately four months. In general, the current procedures are as follows:

1. Applicants participate in a security interview and provide preliminary background information.
2. Every applicant's security information is then forwarded to the FBI and checked on the National Crime Indicator Center (NCIC) computer. Simultaneously, the same information is used to ascertain whether any intelligence files are maintained on the individual.
3. Office of Administration Personnel Management Division arranges to have the applicant tested for illegal drug use.

-more-

Fact Sheet, Page 2

4. If the results of the above inquiries and procedures do not indicate a problem, the new employee has 30 days from the "effective date of hire" to complete the necessary forms for a full background check. If the employee does not complete the form in 30 days, he or she will be put on leave without pay status and access to the complex will be revoked (this guideline was effective as of 3-14-94).
5. Upon receipt of the forms, a security officer reviews them to insure completeness, and then forwards them to the FBI and other relevant authorities.
6. At that point, the employee is eligible for a temporary hard pass. To obtain the pass, the employee must be fingerprinted. The prints are forwarded immediately to the FBI for another computer check. If any problems are identified, the appropriate security office is notified.
7. Generally, within 60 to 90 days of receiving the forms, the FBI submits the results of its background check. The security officer (in consultation with White House Counsel's Office) then reviews the file and addresses any concerns that may have been identified. If there are no concerns (or after any concerns have been resolved), the file is sent to the Secret Service for its review and issuance of a permanent pass.

FACTS

- All EOP staff are within compliance of the Chief of Staff guidelines for employees. These guidelines require all employees to complete security

paperwork within 30 days of employment. Employees on payroll prior to March 1, 1994 and previously not in compliance with the Chief of Staff's guidelines are now in full compliance, including every member of the senior staff.

- In the Executive Office of the President there are 1044 authorized FTEs (Full Time Equivalents) and OGEs (Other Government Employees), excluding OMB and USTR.
- Of the 1044, more than 900 are eligible to be granted access to classified materials on a need to know basis. For the approximately 100 remaining individuals, we are either awaiting FBI background investigations (which generally take 60-90 days) or paperwork because the individual joined the EOP within the last 30 days.
- The Clinton White House has never ordered the U.S. Secret Service to issue a permanent hard pass over their objections.

-more-

Fact Sheet, Page 3

Non-Government Service Passholders/Temporary Hard Passes

- There are fewer than 20 non-government service (NGS) temporary hard passholders. Of these, five are employed or retained by the Democratic National Committee, including Paul Begala, Stan Greenberg, Mandy Grunwald, James Carville, David Wilhelm. Those not employed or retained by the DNC are contractors such as AT&T employees.
- All passholders retained or employed by the DNC will submit to a full FBI background security check, an ethics counseling session, and a security briefing. This is a positive, voluntary step by the White House.
- These advisors do not now, and never have had, access to classified material in the Clinton Administration.

.30-30-30-