

FOIA MARKER

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

Folder Title:

Personnel Security [4]

Staff Office-Individual:

Legal Advisor-Derosa, Mary

Original OA/ID Number:

4058

Row:	Section:	Shelf:	Position:	Stack:
39	6	9	1	v

TO: PRESIDENT

FROM: LAKE

Please File:
E.O.

DOC DATE: 01 AUG 95
SOURCE REF:

KEYWORDS: ACCESS
EO

12968
Personal
Security

INTELLIGENCE

PERSONS:

SUBJECT: EO ON ACCESS TO CLASSIFIED INFO

ACTION: PRESIDENT SGD PER WH EXEC CLERK

DUE DATE: 03 AUG 95 STATUS: C

STAFF OFFICER: APPEL

LOGREF:

FILES: WH

NSCP:

CODES:

D O C U M E N T D I S T R I B U T I O N

FOR ACTION

FOR CONCURRENCE

FOR INFO

APPEL
BASS
BEERS
BERGER
KRECKO
LAKE
NSC CHRON

COMMENTS: _____

DISPATCHED BY _____ DATE _____ BY HAND W/ATTCH

OPENED BY: NSDRS

CLOSED BY: NSDRS

DOC 2 OF 2

UNCLASSIFIED
ACTION DATA SUMMARY REPORT

RECORD ID: 9505901

DOC ACTION OFFICER

CAO ASSIGNED ACTION REQUIRED

001 LAKE	Z 95080111 FOR SIGNATURE
002 PRESIDENT	Z 95080122 FOR SIGNATURE
002	X 95080817 PRESIDENT SGD PER WH EXEC CLERK

DISPATCH DATA SUMMARY REPORT

DOC DATE DISPATCH FOR ACTION

DISPATCH FOR INFO

002 950801	VICE PRESIDENT
002 950801	WH CHIEF OF STAFF

UNCLASSIFIED

Rec'd 8/11/2N

National Security Council
The White House

PROOFED BY: _____

LOG # 5901

URGENT NOT PROOFED: _____

SYSTEM PRS NSC INT

BYPASSED WW DESK: _____

DOCLOG ABK A/O _____

	SEQUENCE TO	INITIAL/DATE	DISPOSITION
<u>15</u> Harmon	<u>1</u>	<u>[Signature]</u>	
Dohse			
Sens			
Soderberg			
Berger	<u>2</u>	<u>sv</u>	<u>Not</u>
Lake	<u>3</u>		
Situation Room		Net Sec Advisor has seen:	
West Wing Desk	<u>4</u>	<u>MC 8/1</u>	<u>[Signature]</u>
Records Mgt.			

A = Action I = Information D = Dispatch R = Retain N = No Further Action

cc:

COMMENTS:

Exec Sec Office has diskette yes

THE WHITE HOUSE

ACTIONWASHINGTON
August 1, 1995

MEMORANDUM FOR THE PRESIDENT

THROUGH: THE EXECUTIVE CLERK

President signed per [Signature] 8/1/95
Executive Clerk

FROM: ANTHONY LAKE ✓

SUBJECT: Executive Order on Access to Classified
InformationPurpose

To recommend that you sign the attached Executive Order.

Background

In the wake of the Ames case and with the support of the Administration, the FY95 Intelligence Authorization Act required the executive branch to establish minimum, uniform standards for access to classified information. It also required that employees with access to particularly sensitive classified information furnish financial and foreign travel information as directed by the President.

Twenty-six executive agencies, industry representatives, the American Bar Association, U.S. Government employee unions and the Congressional intelligence committees actively participated in the drafting and review of the attached order. Judge Mikva and the Deputy Attorney General took particular care to ensure the order reflects this Administration's views on due process and sexual orientation in the clearance process.

Among other things, the order:

- establishes, for the first time, uniform standards for granting clearances throughout the government and requires, with narrow exception, agencies to accept clearances on a reciprocal basis.
- provides that no inference concerning the standards for granting and keeping clearances may be raised solely on the basis of sexual orientation and requires implementing guidelines that are consistent with the FBI's guidelines, which are supported by Barney Frank. Likewise, no negative inference may be raised solely on the basis of mental health counseling, although additional inquiry may be considered where it directly relates to the standards for access.

cc: Vice President
Chief of Staff

-- provides due process protections for persons whose clearances are denied or revoked. (Previous efforts to rewrite the 1950's agency-specific guidelines have failed for lack of consensus over due process provisions.) Your order would require, among other things, a written explanation of the reasons for revocation; an opportunity to request the investigative files without waiting in the FOIA queue, but subject to FOIA privileges; and the right to appeal to a panel comprising at least three persons, two from outside the security field. Agency heads or their deputies, however, would retain authority to exempt procedures if they personally certify that their use could damage national security.

The order also establishes parameters for the submission and review of financial information from employees with regular access to particularly sensitive information (i.e., information on sources and methods, nuclear weapons design or special programs.) Agency heads are given discretion to determine which employees are covered; we anticipate this will range from virtually all employees at CIA to a relative handful at State, Defense and Energy. The order requires financial reports at the time of investigation and reinvestigation (i.e., every five years) and on an annual basis as determined by the head of each agency. Agency heads may use this additional authority as a random check or require it on a wider basis.

The financial disclosure provisions have been a particular concern to contractors, who are covered by the order. While industry associations would clearly prefer to be exempt from the requirement, they were included in the Congressional definition of employee, and we feel many of their concerns can be addressed as they continue to participate in the Security Policy Board's drafting of implementing guidelines and forms. These forms, along with the other guidelines called for by the order, require my concurrence on your behalf.

The order is supported by all participating government agencies, the Office of Management and Budget and by interested members of Congress, industry, the American Bar Association and the government unions and industry representatives who reviewed it.

RECOMMENDATION:

That you sign the Executive Order on Access to Classified Information at Tab A.

Attachment

Tab A Executive Order on Access to Classified Information

WHITE HOUSE STAFFING MEMORANDUM

DATE: August 1 ACTION/CONCURRENCE/COMMENT DUE BY: August 2 9 amSUBJECT: E.O. on Access to Classified Info.

	ACTION	FYI		ACTION	FYI
VICE PRESIDENT	☒	☐	McGINTY	☐	☐
PANETTA	☒	☐	NASH	☐	☐
McLARTY	☐	☐	QUINN	☐	☐
ICKES	☐	☒	RASCO	☐	☐
BOWLES	☐	☒	SOSNIK	☐	☐
RIVLIN	☐	☐	STEPHANOPOULOS	☒	☐
EMANUEL	☐	☐	TYSON	☐	☐
GEARAN	☐	☐	WEBSTER	☐	☐
GIBBONS	☐	☐	WILLIAMS	☐	☐
GRIFFIN	☐	☐	<u>TORKEESON</u>	☒	☐
HALE	☐	☐	<u>M. Scott</u>	☒	☐
HERMAN	☐	☐		☐	☐
HIGGINS	☐	☐		☐	☐
LAKE	☒	☐		☐	☐
LINDSEY	☐	☐		☐	☐
MIKVA	☒	☐		☐	☐
McCURRY	☐	☒		☐	☐

REMARKS:

Please advise. This is time sensitive.

RESPONSE:



EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE OF MANAGEMENT AND BUDGET

WASHINGTON, D.C. 20503

THE DIRECTOR

July 31, 1995

95 JUL 31 P8:33

MEMORANDUM FOR THE PRESIDENT

FROM: Alice M. Rivlin *AMR*
Director

SUBJECT: Proposed Executive Order Entitled "Access to
Classified Information"

SUMMARY: This memorandum forwards for your consideration a proposed Executive order that was prepared by the National Security Council ("NSC"). The proposed order would establish a uniform Federal personnel security program for employees who would be considered for access to classified information.

BACKGROUND: As a result of the Aldrich Ames case, this Administration has taken several actions to strengthen the government's counterintelligence and personnel security programs. On May 3, 1994, you signed Presidential Decision Directive ("PDD") number 24 on Counterintelligence Effectiveness and on September 16, 1994, you signed PDD-29 on Security Policy Coordination. The Intelligence Authorization Act for Fiscal Year 1995 (FY 95) ("Act"), which contained the Administration's legislative proposal to enhance the government's counterintelligence capabilities, became law on October 14, 1994.

Simultaneous with our efforts to seek legislation and take direct Presidential actions through PDD's, NSC began a working group to draft an Executive order to address specific personnel security concerns raised by the Ames case. One such concern was the need for a requirement for government employees with access to particularly sensitive classified information, including the identities of covert U.S. assets, to submit financial disclosure statements. Further, NSC identified the need for such employees to provide their written consent for government access to their financial and consumer information when a valid predicate, such as allegations of espionage, existed.

Congress supported the initial drafts of the proposed order but then legislated through the Act that the President provide a broader order. The broader order would govern access to classified information generally, include uniform minimum requirements governing the scope and frequency of background investigations, and include appeal rights for persons whose access is denied or revoked.

The proposed order would address NSC's original concerns as well as Congress' broader mandate. Initially, employees would not be granted access to classified information unless they: (1) were determined to be eligible for access to classified information based upon an appropriate background investigation; (2) had a demonstrated need-to-know the information (to perform the task); and (3) had signed an approved nondisclosure agreement. For employees that had access to particularly sensitive information such as: (a) the identity of covert agents; (b) technical or specialized national intelligence collection systems; (c) the details or design of code or cryptographic systems; (d) particularly sensitive special access programs; or (e) especially sensitive nuclear weapons design information, the employee could not be granted access to the information unless the employee: (A) filed a financial disclosure report, including information with respect to the spouse and dependent children, as part of the background investigation; (b) agreed to be subject to annual financial disclosure requirements; and (c) filed relevant information concerning foreign travel.

The order would provide that employees who are eligible for access to classified information would be subject to periodic reinvestigations. It would grant appeal rights and minimum adjudicative standards for applicants or employees whose access to classified information was denied or revoked. It would provide reciprocity of clearances among the various agencies.

The SPB, which is given responsibility in the order to develop: (a) a standard financial disclosure form for employees who are given access to particularly sensitive information, (b) a common set of adjudicative guidelines for determining eligibility for access to classified information, (c) a common set of investigative standards for background investigations for access to classified information, (d) minimum investigative standards for granting temporary access to classified information, and (e) a common set of reinvestigation standards, would make their recommendations concerning these responsibilities to the President through the Assistant to the President for National Security Affairs. In developing the standard financial disclosure report for employees who are given access to particularly sensitive information, the SPB would obtain the concurrence of the Director of the Office of Management and Budget.

This order has been carefully drafted and is the product of long and thorough vetting process. None of the affected agencies objects to the proposed Executive order.

RECOMMENDATION: I recommend that you sign the proposed Executive order.

Attachment



U.S. Department of Justice

Office of Legal Counsel

Office of the
Deputy Assistant Attorney General

Washington, DC 20530

July 31, 1995

The President,

The White House.

My dear Mr. President:

I am herewith transmitting a proposed Executive order entitled "Access to Classified Information." This proposed Executive order was prepared by the National Security Council. The Office of Management and Budget, with the approval of the Director, forwarded it to this Department for review with respect to form and legality.

The proposed Executive order is approved with respect to form and legality.

Respectfully,

A handwritten signature in dark ink, appearing to read "R. L. Shiffrin", is written over the typed name.

Richard L. Shiffrin
Deputy Assistant Attorney General



U.S. Department of Justice
Office of Legal Counsel

Office of the
Deputy Assistant Attorney General

Washington, D.C. 20530

July 31, 1995

MEMORANDUM

Re: Proposed Executive Order Entitled
"Access to Classified Information"

The attached proposed Executive order was prepared by the National Security Council ("NSC"). The Office of Management and Budget, with the approval of the Director, forwarded it to this Department for review with respect to form and legality. The proposed order would establish a uniform federal personnel security program for employees who would be considered for access to classified information.

Under the direction of the NSC, a working group was convened to draft an Executive order to address specific security concerns. Among those concerns was the need for a requirement for government employees with access to particularly sensitive classified information to submit financial disclosure statements. This order would address that problem and, more broadly, would govern access to classified information generally, to include uniform minimum requirements governing the scope and frequency of background investigations and appeals rights for persons whose access is denied or revoked. It would also provide for reciprocity of clearances among the various agencies.

The proposed order is approved with respect to form and legality.

Richard L. Shiffrin
Deputy Assistant Attorney General

Executive Order
Access to Classified Information

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information.

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

Part 1

Definitions, Access to Classified Information, Financial Disclosure, and Other Items

Section 1.1. Definitions. For the purposes of this order:

(a) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, the "military departments," as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.

(b) "Applicant" means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

(c) "Authorized investigative agency" means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(d) "Classified information" means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.

(e) "Employee" means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(f) "Foreign power" and "agent of a foreign power" have the meaning provided in 50 U.S.C. 1801.

(g) "Need for access" means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(h) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(i) "Overseas Security Policy Board" means the Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and projects that affect all U.S. Government agencies under the authority of a Chief of Mission.

(j) "Security Policy Board" means the Board established by the President to consider, coordinate, and recommend policy directives for United States security policies, procedures, and practices.

(k) "Special Access Program" has the meaning provided in section 4.1 of Executive Order No. 12958, or any successor order.

Sec. 1.2. Access to Classified Information. (a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Employees shall not be granted access to classified information unless they:

(1) have been determined to be eligible for access under section 3.1 of this order by agency heads or designated officials

based upon a favorable adjudication of an appropriate investigation of the employee's background;

(2) have a demonstrated need-to-know; and

(3) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

(e) (1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of three years thereafter, to:

(A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);

(B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681a); and

(C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where:

(A) there are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(B) information the employing agency deems credible indicates the employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information; or

(C) circumstances indicate the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act, the Fair Credit Reporting Act or any other applicable law.

Sec. 1.3. Financial Disclosure. (a) Not later than 180 days after the effective date of this order, the head of each agency that originates, handles, transmits, or possesses classified information shall designate each employee, by position or category where possible, who has a regular need for access to classified information that, in the discretion of the agency head, would reveal:

(1) the identity of covert agents as defined in the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421);

(2) technical or specialized national intelligence collection and processing systems that, if disclosed in an unauthorized manner, would substantially negate or impair the effectiveness of the system;

(3) the details of (A) the nature, contents, algorithm, preparation, or use of any code, cipher, or cryptographic system or (B) the design, construction, functioning, maintenance, or repair of any cryptographic equipment; but not including information concerning the use of cryptographic equipment and services;

(4) particularly sensitive special access programs, the disclosure of which would substantially negate or impair the effectiveness of the information or activity involved; or

(5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

- (1) files with the head of the agency a financial disclosure report, including information with respect to the spouse and dependent children of the employee, as part of all background investigations or reinvestigations;
- (2) is subject to annual financial disclosure requirements, if selected by the agency head; and
- (3) files relevant information concerning foreign travel, as determined by the Security Policy Board.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

Sec. 1.4. Use of Automated Financial Record Data Bases. As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under \$10,000 that are reported as possible money laundering violations, and records of foreign travel.

Sec. 1.5. Employee Education and Assistance.

The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to:

(a) educate employees about individual responsibilities under this order; and

(b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

Part 2

Access Eligibility Policy and Procedure

Sec. 2.1. Eligibility Determinations. (a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

Sec. 2.2. Level of Access Approval. (a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

(b) Access to classified information relating to a Special Access Program shall be granted in accordance with procedures established by the head of the agency that created the program or, for programs pertaining to intelligence activities (including special activities but not including military operational, strategic, and tactical programs) or intelligence sources and methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

Sec. 2.3 Temporary Access to Higher Levels. (a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

- (1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;
- (2) will not exceed 180 days; and
- (3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) of this section involves another agency's classified information, that agency must concur before access to its information is granted.

Sec. 2.4. Reciprocal Acceptance of Access Eligibility Determinations. (a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a Special Access Program shall not be denied eligibility for access to another Special Access Program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.

(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a Special Access Program or for

candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted under section 2.3 or 3.3 of this order or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the employee access to its information.

Sec. 2.5. Specific Access Requirement. (a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

Sec. 2.6. Access by Non-United States Citizens. (a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information, only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United States government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior ten years of the subject's life can be

appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.

Part 3

Access Eligibility Standards

Sec. 3.1. Standards. (a) No employee shall be deemed to be eligible for access to classified information merely by reason of federal service or contracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(b) Except as provided in section 3.3 and 2.6 of this order, eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall

be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

(c) The United States government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information.

(d) In determining eligibility for access under this order, agencies may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standards in this section may be raised solely on the basis of the sexual orientation of the employee.

(e) No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of subsection (b) of this section are satisfied, and mental health may be considered where it directly relates to those standards.

(f) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of adjudicative guidelines for determining eligibility for access to classified information, including access to Special Access Programs.

Sec. 3.2. Basis for Eligibility Approval. (a) Eligibility determinations for access to classified information shall be

based on information concerning the applicant or employee that is acquired through the investigation conducted pursuant to this order or otherwise available to security officials and shall be made part of the applicants or employee's security record. Applicants or employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access.

(b) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

(c) Nothing in this order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the investigative requirements set forth in this order and its implementing regulations to resolve issues that may arise during the course of a background investigation or reinvestigation.

Sec. 3.3. Special Circumstances. (a) In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited.

(1) Temporary eligibility for access under this section shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately terminated, along with any assignment requiring an access eligibility approval, if such approval is not granted.

(2) Temporary eligibility for access may be granted only by security personnel authorized by the agency head to make access eligibility determinations and shall be based on minimum investigative standards developed by the Security Policy Board not later than 180 days after the effective date of this order.

(3) Temporary eligibility for access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of temporary access.

(b) Nothing in subsection (a) shall be construed as altering the authority of an agency head to waive requirements for granting access to classified information pursuant to statutory authority.

(c) Where access has been terminated under section 2.1(b)(4) of this order and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation as to employees who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior five years, provided they have remained employed by the same employer during the period in question, the employee certifies in writing that there has been no change in the relevant information provided by the employee for the last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by this order for access to classified information.

(d) Access eligibility shall be reapproved for individuals who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior five years and who have been retired or otherwise separated from United States government employment for not more than two years; provided there is no indication the individual may no longer satisfy the

standards of this order, the individual certifies in writing that there has been no change in the relevant information provided by the individual for the last background investigation, and an appropriate record check reveals no unfavorable information.

Sec. 3.4. Reinvestigation Requirements. (a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

(b) Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access established in this order.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

Part 4

Investigations for Foreign Governments

Sec. 4.1. Authority. Agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the United States when requested by a foreign government as part of its own personnel security program and with the consent of the individual.

Part 5

Review of Access Determinations

Sec. 5.1. Determinations of Need for Access. A determination under section 2.1(b)(4) of this order that an employee does not have, or no longer has, a need for access is a discretionary determination and shall be conclusive.

Sec. 5.2. Review Proceedings for Denials or Revocations of Eligibility for Access. (a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of this order shall be:

- (1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit;
- (2) provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act (3 U.S.C. 552A) as applicable, any documents, records, and reports upon which a denial or revocation is based;
- (3) informed of their right to be represented by counsel or other representative at their own expense; to request any documents, records, and reports as described in section 5.2(a)(2) upon which a denial or revocation is based; and to request the entire investigative file, as permitted by the national security and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply;
- (4) provided a reasonable opportunity to reply in writing to, and to request a review of, the determination;
- (5) provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;
- (6) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall comprise at least three members, two of whom shall be

selected from outside the security field. Decisions of the panel shall be in writing, and final except as provided in section (b); and

(7) provided an opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the agency head. A written summary or recording of such appearance shall be made part of the applicant or employee's security record, unless such appearance occurs in the presence of the appeals panel described in section (a)(6).

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in section (a)(6) based upon recommendations from an appeals panel. In such case, the decision of the agency head shall be final.

(c) Agency heads shall promulgate regulations to implement this section and, at their sole discretion and as resources and national security considerations permit, may provide additional review proceedings beyond those required by section (a). This section does not require additional proceedings, however, and creates no procedural or substantive rights.

(d) When the head of an agency or principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This certification shall be conclusive.

(e) This section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to any law or other Executive order to deny or terminate access to classified information in the interests of national security. The power and

responsibility to deny or terminate access to classified information pursuant to any law or other Executive order may be exercised only where the agency head determines that the procedures prescribed in section (a) cannot be invoked in a manner that is consistent with national security. This determination shall be conclusive.

(f) (1) This section shall not be deemed to limit or affect the responsibility and power of an agency head to make determinations of suitability for employment.

(2) Nothing in this section shall require that an agency provide the procedures prescribed in section (a) to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any other reason other than denial of eligibility for access to classified information.

(3) A suitability determination shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information.

Part 6

Implementation

Sec. 6.1. Agency Implementing Responsibilities. Heads of agencies that grant employees access to classified information shall:

(a) designate a senior agency official to direct and administer the agency's personnel security program established by this order. All such programs shall include active oversight and continuing security education and awareness programs to ensure effective implementation of this order;

(b) cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines; and

(c) conduct periodic evaluations of the agency's implementation and administration of this order, including the implementation of section 1.3(a) of this order. Copies of each report shall be provided to the Security Policy Board.

Sec. 6.2. Employee Responsibilities. (a) Employees who are granted eligibility for access to classified information shall:

(1) protect classified information in their custody from unauthorized disclosure;

(2) report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;

(3) report all violations of security regulations to the appropriate security officials; and

(4) comply with all other security requirements set forth in this order and its implementing regulations.

(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

Sec. 6.3. Security Policy Board Responsibilities and Implementation. (a) With respect to actions taken by the

Security Policy Board pursuant to sections 1.3(c), 3.1(f), 3.2(b), 3.3(a)(2), and 3.4(c) of this order, the Board shall make recommendations to the President through the Assistant to the President for National Security Affairs for implementation.

(b) Any guidelines, standards, or procedures developed by the Security Policy Board pursuant to this order shall be consistent with those guidelines issued by the Federal Bureau of Investigation in March 1994 on Background Investigations Policy/Guidelines Regarding Sexual Orientation.

(c) In carrying out its responsibilities under this order, the Security Policy Board shall consult where appropriate with the Overseas Security Policy Board. In carrying out its responsibilities under section 1.3(c) of this order, the Security Policy Board shall obtain the concurrence of the Director of the Office of Management and Budget.

Sec. 6.4. Sanctions. Employees shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for, or allow access to, classified information in violation of this order or its implementing regulations. Sanctions may include reprimand, suspension without pay, removal, and other actions in accordance with applicable law and agency regulations.

Part 7

General Provisions

Sec. 7.1. Classified Information Procedures Act. Nothing in this order is intended to alter the procedures established under the Classified Information Procedures Act (18 U.S.C. App. 1).

Sec. 7.2. General. (a) Information obtained by an agency under sections 1.2(e) or 1.3 of this order may not be disseminated outside the agency, except to:

- (1) the agency employing the employee who is the subject of the records or information;
- (2) the Department of Justice for law enforcement or counterintelligence purposes; or
- (3) any agency if such information is clearly relevant to the authorized responsibilities of such agency.

(b) The Attorney General, at the request of the head of an agency, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) No prior Executive orders are repealed by this order. To the extent that this order is inconsistent with any provision of any prior Executive order, this order shall control, except that this order shall not diminish or otherwise affect the requirements of Executive Order No. 10450, the denial and revocation procedures provided to individuals covered by Executive Order No. 10865, as amended, or access by historical researchers and former presidential appointees under Executive Order No. 12953 or any successor order.

(d) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(e) This Executive order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

(f) This order shall become effective upon publication in the Federal Register.

THE WHITE HOUSE,

Executive Order
Access to Classified Information

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information.

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

Part 1

Definitions, Access to Classified Information, Financial Disclosure, and Other Items

Section 1.1. Definitions. For the purposes of this order:

(a) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, the "military departments," as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.

(b) "Applicant" means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

(c) "Authorized investigative agency" means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(d) "Classified information" means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.

(e) "Employee" means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(f) "Foreign power" and "agent of a foreign power" have the meaning provided in 50 U.S.C. 1801.

(g) "Need for access" means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(h) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(i) "Overseas Security Policy Board" means the Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and projects that affect all U.S. Government agencies under the authority of a Chief of Mission.

(j) "Security Policy Board" means the Board established by the President to consider, coordinate, and recommend policy directives for United States security policies, procedures, and practices.

(k) "Special Access Program" has the meaning provided in section 4.1 of Executive Order No. 12958, or any successor order.

Sec. 1.2. Access to Classified Information. (a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Employees shall not be granted access to classified information unless they:

(1) have been determined to be eligible for access under section 3.1 of this order by agency heads or designated officials

based upon a favorable adjudication of an appropriate investigation of the employee's background;

(2) have a demonstrated need-to-know; and

(3) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

(e)(1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of three years thereafter, to:

(A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);

(B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681a); and

(C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where:

(A) there are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(B) information the employing agency deems credible indicates the employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information; or

(C) circumstances indicate the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act, the Fair Credit Reporting Act or any other applicable law.

Sec. 1.3. Financial Disclosure. (a) Not later than 180 days after the effective date of this order, the head of each agency that originates, handles, transmits, or possesses classified information shall designate each employee, by position or category where possible, who has a regular need for access to classified information that, in the discretion of the agency head, would reveal:

(1) the identity of covert agents as defined in the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421);

(2) technical or specialized national intelligence collection and processing systems that, if disclosed in an unauthorized manner, would substantially negate or impair the effectiveness of the system;

(3) the details of (A) the nature, contents, algorithm, preparation, or use of any code, cipher, or cryptographic system or (B) the design, construction, functioning, maintenance, or repair of any cryptographic equipment; but not including information concerning the use of cryptographic equipment and services;

(4) particularly sensitive special access programs, the disclosure of which would substantially negate or impair the effectiveness of the information or activity involved; or

(5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

(1) files with the head of the agency a financial disclosure report, including information with respect to the spouse and dependent children of the employee, as part of all background investigations or reinvestigations;

(2) is subject to annual financial disclosure requirements, if selected by the agency head; and

(3) files relevant information concerning foreign travel, as determined by the Security Policy Board.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

Sec. 1.4. Use of Automated Financial Record Data Bases. As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under \$10,000 that are reported as possible money laundering violations, and records of foreign travel.

Sec. 1.5. Employee Education and Assistance.

The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to:

(a) educate employees about individual responsibilities under this order; and

(b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

Part 2

Access Eligibility Policy and Procedure

Sec. 2.1. Eligibility Determinations. (a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

Sec. 2.2. Level of Access Approval. (a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

(b) Access to classified information relating to a Special Access Program shall be granted in accordance with procedures established by the head of the agency that created the program or, for programs pertaining to intelligence activities (including special activities but not including military operational, strategic, and tactical programs) or intelligence sources and methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

Sec. 2.3 Temporary Access to Higher Levels. (a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

- (1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;
- (2) will not exceed 180 days; and
- (3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) of this section involves another agency's classified information, that agency must concur before access to its information is granted.

Sec. 2.4. Reciprocal Acceptance of Access Eligibility Determinations. (a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a Special Access Program shall not be denied eligibility for access to another Special Access Program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.

(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a Special Access Program or for

candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted under section 2.3 or 3.3 of this order or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the employee access to its information.

Sec. 2.5. Specific Access Requirement. (a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

Sec. 2.6. Access by Non-United States Citizens. (a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information, only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United States government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior ten years of the subject's life can be

appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.

Part 3

Access Eligibility Standards

Sec. 3.1. Standards. (a) No employee shall be deemed to be eligible for access to classified information merely by reason of federal service or contracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(b) Except as provided in section 3.3 and 2.6 of this order, eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall

be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

(c) The United States government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information.

(d) In determining eligibility for access under this order, agencies may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standards in this section may be raised solely on the basis of the sexual orientation of the employee.

(e) No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of subsection (b) of this section are satisfied, and mental health may be considered where it directly relates to those standards.

(f) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of adjudicative guidelines for determining eligibility for access to classified information, including access to Special Access Programs.

Sec. 3.2. Basis for Eligibility Approval. (a) Eligibility determinations for access to classified information shall be

based on information concerning the applicant or employee that is acquired through the investigation conducted pursuant to this order or otherwise available to security officials and shall be made part of the applicants or employee's security record. Applicants or employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access.

(b) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

(c) Nothing in this order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the investigative requirements set forth in this order and its implementing regulations to resolve issues that may arise during the course of a background investigation or reinvestigation.

Sec. 3.3. Special Circumstances. (a) In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited.

(1) Temporary eligibility for access under this section shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately terminated, along with any assignment requiring an access eligibility approval, if such approval is not granted.

(2) Temporary eligibility for access may be granted only by security personnel authorized by the agency head to make access eligibility determinations and shall be based on minimum investigative standards developed by the Security Policy Board not later than 180 days after the effective date of this order.

(3) Temporary eligibility for access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of temporary access.

(b) Nothing in subsection (a) shall be construed as altering the authority of an agency head to waive requirements for granting access to classified information pursuant to statutory authority.

(c) Where access has been terminated under section 2.1(b)(4) of this order and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation as to employees who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior five years, provided they have remained employed by the same employer during the period in question, the employee certifies in writing that there has been no change in the relevant information provided by the employee for the last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by this order for access to classified information.

(d) Access eligibility shall be reapproved for individuals who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior five years and who have been retired or otherwise separated from United States government employment for not more than two years; provided there is no indication the individual may no longer satisfy the

standards of this order, the individual certifies in writing that there has been no change in the relevant information provided by the individual for the last background investigation, and an appropriate record check reveals no unfavorable information.

Sec. 3.4. Reinvestigation Requirements. (a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

(b) Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access established in this order.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

Part 4

Investigations for Foreign Governments

Sec. 4.1. Authority. Agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the United States when requested by a foreign government as part of its own personnel security program and with the consent of the individual.

Part 5

Review of Access Determinations

Sec. 5.1. Determinations of Need for Access. A determination under section 2.1(b)(4) of this order that an employee does not have, or no longer has, a need for access is a discretionary determination and shall be conclusive.

Sec. 5.2. Review Proceedings for Denials or Revocations of Eligibility for Access. (a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of this order shall be:

(1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit;

(2) provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act (3 U.S.C. 552A) as applicable, any documents, records, and reports upon which a denial or revocation is based;

(3) informed of their right to be represented by counsel or other representative at their own expense; to request any documents, records, and reports as described in section 5.2(a)(2) upon which a denial or revocation is based; and to request the entire investigative file, as permitted by the national security and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply;

(4) provided a reasonable opportunity to reply in writing to, and to request a review of, the determination;

(5) provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

(6) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall be comprised of at least three members, two of whom shall be

selected from outside the security field. Decisions of the panel shall be in writing, and final except as provided in section (b); and

(7) provided an opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the agency head. A written summary or recording of such appearance shall be made part of the applicant or employee's security record, unless such appearance occurs in the presence of the appeals panel described in section (a)(6).

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in section (a)(6) based upon recommendations from an appeals panel. In such case, the decision of the agency head shall be final.

(c) Agency heads shall promulgate regulations to implement this section and, at their sole discretion and as resources and national security considerations permit, may provide additional review proceedings beyond those required by section (a). This section does not require additional proceedings, however, and creates no procedural or substantive rights.

(d) When the head of an agency or principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This certification shall be conclusive.

(e) This section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to any law or other Executive order to deny or terminate access to classified information in the interests of national security. The power and

responsibility to deny or terminate access to classified information pursuant to any law or other Executive order may be exercised only where the agency head determines that the procedures prescribed in section (a) cannot be invoked in a manner that is consistent with national security. This determination shall be conclusive.

(f) (1) This section shall not be deemed to limit or affect the responsibility and power of an agency head to make determinations of suitability for employment.

(2) Nothing in this section shall require that an agency provide the procedures prescribed in section (a) to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any other reason other than denial of eligibility for access to classified information.

(3) A suitability determination shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information.

Part 6

Implementation

Sec. 6.1. Agency Implementing Responsibilities. Heads of agencies that grant employees access to classified information shall:

(a) designate a senior agency official to direct and administer the agency's personnel security program established by this order. All such programs shall include active oversight and continuing security education and awareness programs to ensure effective implementation of this order;

(b) cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines; and

(c) conduct periodic evaluations of the agency's implementation and administration of this order, including the implementation of section 1.3(a) of this order. Copies of each report shall be provided to the Security Policy Board.

Sec. 6.2. Employee Responsibilities. (a) Employees who are granted eligibility for access to classified information shall:

- (1) protect classified information in their custody from unauthorized disclosure;
- (2) report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;
- (3) report all violations of security regulations to the appropriate security officials; and
- (4) comply with all other security requirements set forth in this order and its implementing regulations.

(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

Sec. 6.3. Security Policy Board Responsibilities and Implementation. (a) With respect to actions taken by the Security Policy Board pursuant to sections 1.3(c), 3.1(f), 3.2(b), 3.3(a)(2), and 3.4(c) of this order, the Board shall make recommendations to the President through the Assistant to the President for National Security Affairs for implementation.

(b) Any guidelines, standards, or procedures developed by the Security Policy Board pursuant to this order shall be consistent with those guidelines issued by the Federal Bureau of Investigation in March 1994 on Background Investigations Policy/Guidelines Regarding Sexual Orientation.

(c) In carrying out its responsibilities under this order, the Security Policy Board shall consult where appropriate with the Overseas Security Policy Board. In carrying out its responsibilities under section 1.3(c) of this order, the Security Policy Board shall obtain the concurrence of the Director of the Office of Management and Budget.

Sec. 6.4. Sanctions. Employees shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for, or allow access to, classified information in violation of this order or its implementing regulations. Sanctions may include reprimand, suspension without pay, removal, and other actions in accordance with applicable law and agency regulations.

Part 7

General Provisions

Sec. 7.1. Classified Information Procedures Act. Nothing in this order is intended to alter the procedures established under the Classified Information Procedures Act (18 U.S.C. App. 1).

Sec. 7.2. General. (a) Information obtained by an agency under sections 1.2(e) or 1.3 of this order may not be disseminated outside the agency, except to:

- (1) the agency employing the employee who is the subject of the records or information;
- (2) the Department of Justice for law enforcement or counterintelligence purposes; or
- (3) any agency if such information is clearly relevant to the authorized responsibilities of such agency.

(b) The Attorney General, at the request of the head of an agency, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) No prior Executive orders are repealed by this order. To the extent that this order is inconsistent with any provision of any prior Executive order, this order shall control, except that this order shall not diminish or otherwise affect the requirements of Executive Order No. 10450, the denial and revocation procedures provided to individuals covered by Executive Order No. 10865, as amended, or access by historical researchers and former presidential appointees under Executive Order No. 12958 or any successor order.

(d) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(e) This Executive order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

(f) This order shall become effective upon publication in the Federal Register.

THE WHITE HOUSE,

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

5901

July 31, 1995

ACTION

MEMORANDUM FOR ANTHONY LAKE

THROUGH: R. RAND BEERS
FROM: EDWARD J. APPEL
SUBJECT: Executive Order on Access to Classified
Information

Attached at Tab A is a memorandum for the President, recommending that he sign the Executive Order on Access to Classified Information.

As you are aware, the Security Policy Board and National Security Council staff have been drafting this order since October, 1994. Since March, 1995, additional refinements have been added to address due process concerns. The draft was produced with the collaboration of the government's security intelligentsia, vetted by all relevant agencies and reviewed by the Intelligence Committees, Secrecy Commission, American Bar Association, government unions, industry associations and OMB.

While industry is still worried about the financial disclosure provisions (and agencies about the cost of implementation), they have been consulted throughout the process. Industry comments will also be sought as the Security Policy Board prepares its recommendations, as required by the order. Those recommendations, including draft financial disclosure forms, standards and guidelines, will be sent to the White House for approval, prior to being promulgated.

The order is summarized in the attached memo to the President.

Concurrence by: Alan Kreczko *AK*

RECOMMENDATION:

That you sign the memo to the President, recommending that he sign the Executive Order on Access to Classified Information.

Attachments

Tab I Memo for the President
Tab A Executive Order