

FOIA MARKER

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

Folder Title:

[HPSCI Document Request re: WH Security Clearances, 1997] [1]

Staff Office-Individual:

Staff Director-Soderberg, Nancy

Original OA/ID Number:

1421B

Row:	Section:	Shelf:	Position:	Stack:
50	2	4	3	V

Withdrawal/Redaction Sheet

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
--------------------------	---------------	------	-------------

001. paper	Security Procedures for the EOP Security Office. (23 pages)	11/1996	b(7)(E), b(7)(F)
------------	---	---------	------------------

COLLECTION:

Clinton Presidential Records
National Security Council
Staff Director (Nancy Soderberg)
OA/Box Number: 1421B

FOLDER TITLE:

[HSPCI Document Request re: WH Security Clearances, 1997] [1]

2006-1066-F

vz884

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

THE WHITE HOUSE
WASHINGTON

JB

August 4, 1997

BY HAND DELIVERY

Patrick B. Murray
Chief Counsel
Chris Barton
Deputy Chief Counsel
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, DC 20515-6415

Dear Patrick and Chris:

Following up on our prior discussions, I am writing in response to the Committee's June 24, 1997 letter to Mr. Charles F.C. Ruff, Counsel to the President. In that letter, the Committee requests information concerning the Administration's policies and procedures governing access to classified information. The Committee has also requested a listing of White House staff and National Security Council (NSC) employees who have been cleared for access to classified information during this Administration. This letter responds to those requests.

Access to classified information is governed by Executive Order 12968, which is attached at Tab A. The Executive Order became effective August 2, 1995 and was intended to establish a uniform procedure and program regarding access to classified information. The Executive Office of the President (EOP) Security Office handles administration of the Executive Order for the White House, with the exception of the NSC, as discussed below. The EOP Security Office, overseen by EOP Security Officer Charles C. Easley, currently utilizes the Security Procedures for the EOP Security Office, a copy of which is behind Tab B. The Security Procedures manual provides the administrative framework for implementing the Executive Order and describes the general procedures concerning the decision-making process. In making individual adjudicative determinations, the EOP Security Office utilizes the Adjudicative Guidelines as recently promulgated by the Security Policy Board. A copy of those guidelines is attached at Tab C.

Patrick B. Murray, Esq.
Chris Barton, Esq.
August 4, 1997
Page 2

The NSC has historically operated and continues to operate its own regime governing access to classified information separate from the EOP Security Office. It is a condition of employment at the NSC to have a Top Secret Clearance and Sensitive Compartmented Information (SCI) access. The NSC utilizes the Adjudicative Guidelines of the Security Policy Board, mentioned above, and SCI clearances are approved pursuant to the procedures of Directive No. 1/14 of the Director of Central Intelligence, attached at Tab D.

With respect to components of the EOP apart from the NSC, in past administrations, and for the first several years of this Administration, the procedure and criteria for obtaining a permanent building pass (or "Blue Pass") were the same to determine security clearance eligibility. Individuals whose completed Background Investigations were favorably adjudicated, and who thereby obtained a permanent Blue Pass, were deemed to be capable of receiving classified information through the Top Secret level on a need-to-know basis as determined by their supervisor.

As part of implementing President Clinton's Executive Order 12968 and improving security procedures, beginning in late 1995 the security clearance procedure was formalized and the Blue Pass determination was decoupled from the clearance determination. White House employees who were determined to require a security clearance were granted formal security clearances by the EOP Security Office and completed SF-312 nondisclosure agreements. Under this regime, as discussed in the Security Procedures manual, the head of the individual's employing office indicates what level of clearance, if any, is required once a completed Background Investigation is favorably adjudicated. Moreover, as part of this formalization, an effort was made to assess systematically which employees actually were in need of continued security clearances. Two memoranda relating to this continuing effort are attached at Tab E.

It should be noted that the Office of the Vice President instituted its own formal security clearance procedures prior to the implementation of President Clinton's Executive Order. The memorandum attached at Tab F describes the regime followed by the Vice President's Office for a period before the transition. As part of implementation of the Executive Order, the Vice President's Office now utilizes the mechanisms of the EOP Security Office to grant clearances to the Vice President's staff. The memorandum attached at Tab G describes the current procedures in place in the Vice President's office. With respect to the Vice President's National Security Advisor's office (NSA), wherein most staff members are detailees from other agencies and come to the NSA with security clearances granted by their home agency, they still must have a TS/SCI clearance granted by the EOP Security Office (in conjunction with the CIA). It should be noted that, in the case of certain short-term detailees (like Presidential Management Interns), the EOP Security Office will accept the home agency's certification of the detailee's

Patrick B. Murray, Esq.
Chris Barton, Esq.
August 4, 1997
Page 3

clearance status. The EOP Security Office administers the security clearance procedures for the NSA, with the exception of a pre-employment screening interview that the White House Military Office conducts of all active-duty members of the military who are being considered for a job at the NSA. (This screening interview process also occurs for the stewards and drivers at the Vice President's residence and the two Military Aides who travel with the Vice President.)

Pursuant to the Committee's request, I am enclosing at Tab H a list of employees of the White House Office (WHO), Office of the Vice President (VPO), and the Office of Policy Development (OPD) who have been cleared through the formal procedures described above. (It should be noted that many of these individuals no longer work at the White House.) The date next to an individual's name signifies the date on which the Security Office formally granted the individual a security clearance (and not the date of employment). Absent from the Office of the Vice President's listing are employees of the Vice President's NSA office other than Douglas Babcock, Darrien Boulton, Leon Fuerth, and David Perkins. While all NSA employees must have an SCI clearance granted by the Security Office, most of them are employees of other agencies detailed to the NSA rather than White House employees. A complete list of the individuals who have worked at the NSA from January 1993 to present is attached at Tab I. Finally, a list of all employees of the NSC from 1993 to present is attached at Tab J. As mentioned, it is a condition of employment for all NSC employees to obtain a TS/SCI clearance. The Security Office list and the NSC list are computer-generated printouts; we have endeavored to ensure the accuracy of these printouts, but, in light of our desire to provide information to the Committee promptly, we have not had the opportunity to review systematically every name on the lists to ensure complete accuracy. Similarly, the Vice President's NSA office list was generated from NSA records; it is complete to the best of our knowledge, but again, we cannot attest to its absolute accuracy.

I hope the above information and attached materials are helpful to the Committee. I look forward to working with the Committee as its investigation proceeds. If you have any questions, please feel free to contact me at 456-6243.

Sincerely,

A handwritten signature in dark ink, appearing to read "Michael X. Imbroscio", with a long horizontal flourish extending to the right.

Michael X. Imbroscio
Associate Counsel to the President

cc: Michael W. Sheehy, Esq.

ARNOLD & PORTER

555 TWELFTH STREET, N.W.
WASHINGTON, D.C. 20004-1206

(202) 942-5000
FACSIMILE: (202) 942-5999

JACK QUINN
(202) 942-5027

NEW YORK
DENVER
LOS ANGELES
LONDON

July 22, 1997

The Honorable Porter J. Goss
Chairman
The Honorable Norman D. Dicks
Ranking Democratic Member
Permanent Select Committee on Intelligence
U.S. House of Representatives
Room H-405, U.S. Capitol
Washington, D.C. 20515-6415

Dear Chairman Goss and Representative Dicks:

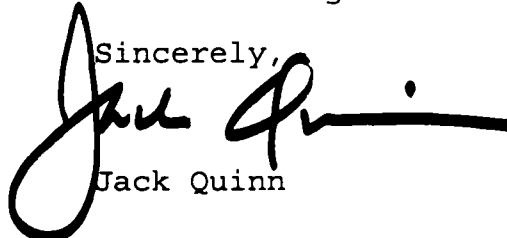
I received your July 8, 1997 letter requesting that I contact your staff regarding your committee's inquiry into Executive Branch clearance procedures for granting access to intelligence information.

I understand that you also have contacted the White House Counsel's office about these matters directly, and that the White House is engaged in discussions with your staff about how it can best be responsive to your request.

As such, I believe that current Administration officials will be in a position to answer your questions in a comprehensive fashion, including with respect to the procedures and policies that were in effect for White House staff during my tenure as Counsel to the President.

I will remain in touch with White House Counsel staff about this matter and await their further guidance.

Sincerely,

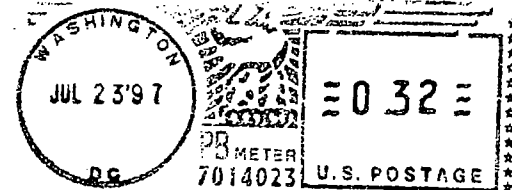
A handwritten signature in black ink, appearing to read "Jack Quinn", with a large, stylized loop at the end.

Jack Quinn

bcc: Charles Ruff
Alan Kreczko ✓

ARNOLD & PORTER

555 TWELFTH STREET, N.W.
WASHINGTON, D.C. 20004-1202



Alan Kreczko
The White House
Washington, D.C. 20500

PORTER J. GOSS, FLORIDA, CHAIRMAN

C.W. BILL YOUNG, FLORIDA
JERRY LEWIS, CALIFORNIA
BUD SHUSTER, PENNSYLVANIA
BILL MCCOLLUM, FLORIDA
MICHAEL N. CASTLE, DELAWARE
SHERWOOD L. BOEHLERT, NEW YORK
CHARLES F. BASS, NEW HAMPSHIRE
JIM GIBBONS, NEVADA

NORMAN D. DICKS, WASHINGTON
JULIAN C. DIXON, CALIFORNIA
DAVID E. SKAGGS, COLORADO
NANCY PELOSI, CALIFORNIA
JANE HARMAN, CALIFORNIA
IKE SKELTON, MISSOURI
SANFORD D. BISHOP, JR., GEORGIA

NEWT GINGRICH, GEORGIA, EX OFFICIO
RICHARD A. GEPHARDT, MISSOURI, EX OFFICIO

ROOM M-406, U.S. CAPITOL
(202) 225-4121

JOHN L. MILLS, STAFF DIRECTOR
PATRICK B. MURRAY, CHIEF COUNSEL
MICHAEL W. SHEEHY, DEMOCRATIC COUNSEL

U.S. HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE

ON INTELLIGENCE

WASHINGTON, DC 20515-6415

J

July 8, 1997

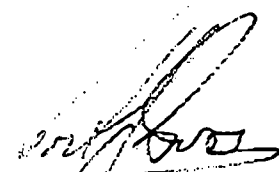
Mr. Jack M. Quinn
Arnold & Porter
555 12th Street, N.W.
12th Floor
Washington, D.C. 20004

Dear Mr. Quinn:

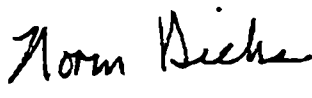
The House Permanent Select Committee on Intelligence is currently investigating allegations of improper access to intelligence information and Executive Branch clearance procedures for granting such access (see attached press release). We believe that your experience as Counsel to President Clinton will aid the Committee's investigation and assist us in establishing which procedures and policies were in effect for White House staff during your tenure.

We would appreciate your allowing our staff an opportunity to meet with you to discuss these and any related issues. Please contact Chris Barton, Deputy Chief Counsel, at 202-225-4121, to arrange a mutually convenient meeting time, or to discuss any questions regarding this matter that you might have.

Sincerely,



Porter J. Goss
Chairman



Norman D. Dicks
Ranking Democratic Member

Enclosure

LARRY COMBEST, TEXAS, CHAIRMAN

ROBERT K. DORNAN, CALIFORNIA

C.W. BILL YOUNG, FLORIDA

JAMES V. HANSEN, UTAH

JERRY LEWIS, CALIFORNIA

PORTER J. GOSSE, FLORIDA

BUO SHUSTER, PENNSYLVANIA

BILL MCCOLLUM, FLORIDA

MICHAEL N. CASTLE, DELAWARE

NORMAN D. DICKS, WASHINGTON

BILL RICHARDSON, NEW MEXICO

JULIAN C. DIXON, CALIFORNIA

ROBERT G. TORRICELLI, NEW JERSEY

DAVID E. SKAGGS, COLORADO

NANCY PELOSI, CALIFORNIA

JANE HARMAN, CALIFORNIA

NEWT GINGRICH, GEORGIA, EX OFFICIO

RICHARD A. GEPHARDT, MISSOURI, EX OFFICIO

ROOM 4-405, U.S. CAPITOL
(202) 225-4121MARK M. LOWENTHAL, STAFF DIRECTOR
LOUIS H. DUPART, CHIEF COUNSEL
MICHAEL W. SHEEHY, DEMOCRATIC COUNSEL

U.S. HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE

ON INTELLIGENCE

WASHINGTON, DC 20515-6415

STATEMENT OF THE COMMITTEE

REGARDING ITS INQUIRY:

"ACCESS TO INTELLIGENCE INFORMATION

AND

EXECUTIVE BRANCH CLEARANCE PROCEDURES"

MARCH 5, 1997

The House Permanent Select Committee on Intelligence (HPSCI) today formally opened an inquiry into issues relating to the process of protecting access to intelligence information in the Executive Branch and whether elements of foreign governments attempted to influence domestic political campaigns since 1992.

The scope of the investigation – titled "Access to Intelligence Information and Executive Branch Clearance Procedures" – is as follows:

- I. Whether procedures governing the issuance of clearances for access to intelligence information issued since January 20, 1993 within the Executive Branch have been appropriate and properly administered.
- II. Whether adequate and proper security controls have been maintained over classified intelligence information which has been provided to or briefed to executive Branch employees or former employees.
- III. Whether elements of foreign governments have engaged in an effort to illegally influence U.S. domestic political campaigns since November 1992.
- IV. In conjunction with items I-III, whether any Executive Branch employee or former employee acted improperly to affect adversely U.S. intelligence collection or dissemination decisions.

The HPSCI will conduct a full and thorough investigation on these matters, which are within its jurisdiction. As always, it will operate within the constraints of Committee and House rules, which are designed to protect the security of classified information and which require a formal vote of the Committee to release such information publicly.

PORTER J. GOSS, FLORIDA, CHAIRMAN

C.W. BILL YOUNG, FLORIDA
JERRY LEWIS, CALIFORNIA
BUO SHUSTER, PENNSYLVANIA
BILL MCCOLLUM, FLORIDA
MICHAEL N. CASTLE, DELAWARE
SHERWOOD L. BOEHLERT, NEW YORK
CHARLES F. BASS, NEW HAMPSHIRE
JIM GIBBONS, NEVADA

NORMAN D. DICKS, WASHINGTON
JULIAN C. DIXON, CALIFORNIA
DAVID E. SKAGGS, COLORADO
NANCY PELOSI, CALIFORNIA
JANE HARMAN, CALIFORNIA
IKE SKELTON, MISSOURI
SANFORD D. BISHOP, JR., GEORGIA

NEWT GINGRICH, GEORGIA, EX OFFICIO
RICHARD A. GEPHARDT, MISSOURI, EX OFFICIO

Room H-405, U.S. CAPITOL
(202) 225-4121

JOHN I. MILLIS, STAFF DIRECTOR
PATRICK S. MURRAY, CHIEF COUNSEL
MICHAEL W. SHEEHY, DEMOCRATIC COUNSEL

U.S. HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE

ON INTELLIGENCE

WASHINGTON, DC 20515-8415

June 17, 1997

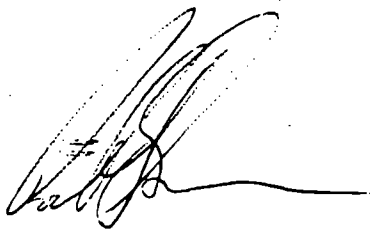
Mr. Anthony Lake
2501 Calvert Street, N.W.
Apartment 805
Washington, D.C. 20008

Dear Mr. Lake:

The House Permanent Select Committee on Intelligence is currently investigating allegations of improper access to intelligence information and Executive Branch clearance procedures for granting such access (see attached press release). We believe that your experience as National Security Advisor to President Clinton will aid the Committee's investigation and assist us in establishing which procedures and policies were in effect for White House staff during your tenure.

We would appreciate your allowing our staff an opportunity to meet with you to discuss these and any related issues. Please contact Chris Barton, Deputy Chief Counsel, at 202-225-4121, to arrange a mutually convenient meeting time, or to discuss any questions regarding this matter that you might have.

Sincerely,



Porter J. Goss
Chairman



Norman D. Dicks
Ranking Democratic Member

Enclosure

HARRY COMBEST, TEXAS, CHAIRMAN

ROBERT K. DORNAN, CALIFORNIA
C.W. BILL YOUNG, FLORIDA
JAMES V. HANSEN, UTAH
JERRY LEWIS, CALIFORNIA
PORTER J. GOSS, FLORIDA
BUD SHUSTER, PENNSYLVANIA
BILL MCCOLLUM, FLORIDA
MICHAEL N. CASTLE, DELAWARE

NORMAN D. DICKS, WASHINGTON
BILL RICHARDSON, NEW MEXICO
JULIAN C. DIXON, CALIFORNIA
ROBERT G. TORRICELLI, NEW JERSEY
DAVID E. SKAGGS, COLORADO
NANCY PELOSI, CALIFORNIA
JANE HARMAN, CALIFORNIA

NEWT GINGRICH, GEORGIA, EX OFFICIO
RICHARD A. GEPHARDT, MISSOURI, EX OFFICIO

ROOM H-405, U.S. CAPITOL
(202) 225-4121

MARK M. LOWENTHAL, STAFF DIRECTOR
LOUIS H. DUPART, CHIEF COUNSEL
MICHAEL W. SKEEHY, DEMOCRATIC COUNSEL

U.S. HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE
WASHINGTON, DC 20515-6415

STATEMENT OF THE COMMITTEE
REGARDING ITS INQUIRY:
"ACCESS TO INTELLIGENCE INFORMATION
AND
EXECUTIVE BRANCH CLEARANCE PROCEDURES"
MARCH 5, 1997

The House Permanent Select Committee on Intelligence (HPSCI) today formally opened an inquiry into issues relating to the process of protecting access to intelligence information in the Executive Branch and whether elements of foreign governments attempted to influence domestic political campaigns since 1992.

The scope of the investigation – titled "Access to Intelligence Information and Executive Branch Clearance Procedures" – is as follows:

- I. Whether procedures governing the issuance of clearances for access to intelligence information issued since January 20, 1993 within the Executive Branch have been appropriate and properly administered.
- II. Whether adequate and proper security controls have been maintained over classified intelligence information which has been provided to or briefed to executive Branch employees or former employees.
- III. Whether elements of foreign governments have engaged in an effort to illegally influence U.S. domestic political campaigns since November 1992.
- IV. In conjunction with items I-III, whether any Executive Branch employee or former employee acted improperly to affect adversely U.S. intelligence collection or dissemination decisions.

The HPSCI will conduct a full and thorough investigation on these matters, which are within its jurisdiction. As always, it will operate within the constraints of Committee and House rules, which are designed to protect the security of classified information and which require a formal vote of the Committee to release such information publicly.

THE WHITE HOUSE
WASHINGTON

August 4, 1997

BY HAND DELIVERY

Patrick B. Murray
Chief Counsel
Chris Barton
Deputy Chief Counsel
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, DC 20515-6415

Dear Patrick and Chris:

Following up on our prior discussions, I am writing in response to the Committee's June 24, 1997 letter to Mr. Charles F.C. Ruff, Counsel to the President. In that letter, the Committee requests information concerning the Administration's policies and procedures governing access to classified information. The Committee has also requested a listing of White House staff and National Security Council (NSC) employees who have been cleared for access to classified information during this Administration. This letter responds to those requests.

Access to classified information is governed by Executive Order 12968, which is attached at Tab A. The Executive Order became effective August 2, 1995 and was intended to establish a uniform procedure and program regarding access to classified information. The Executive Office of the President (EOP) Security Office handles administration of the Executive Order for the White House, with the exception of the NSC, as discussed below. The EOP Security Office, overseen by EOP Security Officer Charles C. Easley, currently utilizes the Security Procedures for the EOP Security Office, a copy of which is behind Tab B. The Security Procedures manual provides the administrative framework for implementing the Executive Order and describes the general procedures concerning the decision-making process. In making individual adjudicative determinations, the EOP Security Office utilizes the Adjudicative Guidelines as recently promulgated by the Security Policy Board. A copy of those guidelines is attached at Tab C.

Patrick B. Murray, Esq.
Chris Barton, Esq.
August 4, 1997
Page 2

The NSC has historically operated and continues to operate its own regime governing access to classified information separate from the EOP Security Office. It is a condition of employment at the NSC to have a Top Secret Clearance and Sensitive Compartmented Information (SCI) access. The NSC utilizes the Adjudicative Guidelines of the Security Policy Board, mentioned above, and SCI clearances are approved pursuant to the procedures of Directive No. 1/14 of the Director of Central Intelligence, attached at Tab D.

With respect to components of the EOP apart from the NSC, in past administrations, and for the first several years of this Administration, the procedure and criteria for obtaining a permanent building pass (or "Blue Pass") were the same to determine security clearance eligibility. Individuals whose completed Background Investigations were favorably adjudicated, and who thereby obtained a permanent Blue Pass, were deemed to be capable of receiving classified information through the Top Secret level on a need-to-know basis as determined by their supervisor.

As part of implementing President Clinton's Executive Order 12968 and improving security procedures, beginning in late 1995 the security clearance procedure was formalized and the Blue Pass determination was decoupled from the clearance determination. White House employees who were determined to require a security clearance were granted formal security clearances by the EOP Security Office and completed SF-312 nondisclosure agreements. Under this regime, as discussed in the Security Procedures manual, the head of the individual's employing office indicates what level of clearance, if any, is required once a completed Background Investigation is favorably adjudicated. Moreover, as part of this formalization, an effort was made to assess systematically which employees actually were in need of continued security clearances. Two memoranda relating to this continuing effort are attached at Tab E.

It should be noted that the Office of the Vice President instituted its own formal security clearance procedures prior to the implementation of President Clinton's Executive Order. The memorandum attached at Tab F describes the regime followed by the Vice President's Office for a period before the transition. As part of implementation of the Executive Order, the Vice President's Office now utilizes the mechanisms of the EOP Security Office to grant clearances to the Vice President's staff. The memorandum attached at Tab G describes the current procedures in place in the Vice President's office. With respect to the Vice President's National Security Advisor's office (NSA), wherein most staff members are detailees from other agencies and come to the NSA with security clearances granted by their home agency, they still must have a TS/SCI clearance granted by the EOP Security Office (in conjunction with the CIA). It should be noted that, in the case of certain short-term detailees (like Presidential Management Interns), the EOP Security Office will accept the home agency's certification of the detailee's

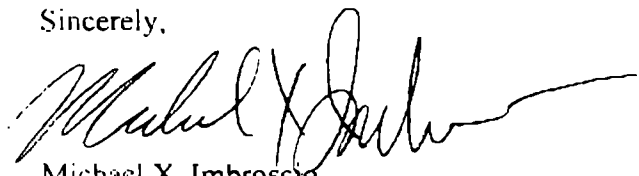
Patrick B. Murray, Esq.
Chris Barton, Esq.
August 4, 1997
Page 3

clearance status. The EOP Security Office administers the security clearance procedures for the NSA, with the exception of a pre-employment screening interview that the White House Military Office conducts of all active-duty members of the military who are being considered for a job at the NSA. (This screening interview process also occurs for the stewards and drivers at the Vice President's residence and the two Military Aides who travel with the Vice President.)

Pursuant to the Committee's request, I am enclosing at Tab H a list of employees of the White House Office (WHO), Office of the Vice President (VPO), and the Office of Policy Development (OPD) who have been cleared through the formal procedures described above. (It should be noted that many of these individuals no longer work at the White House.) The date next to an individual's name signifies the date on which the Security Office formally granted the individual a security clearance (and not the date of employment). Absent from the Office of the Vice President's listing are employees of the Vice President's NSA office other than Douglas Babcock, Darrien Boulton, Leon Fuerth, and David Perkins. While all NSA employees must have an SCI clearance granted by the Security Office, most of them are employees of other agencies detailed to the NSA rather than White House employees. A complete list of the individuals who have worked at the NSA from January 1993 to present is attached at Tab I. Finally, a list of all employees of the NSC from 1993 to present is attached at Tab J. As mentioned, it is a condition of employment for all NSC employees to obtain a TS/SCI clearance. The Security Office list and the NSC list are computer-generated printouts; we have endeavored to ensure the accuracy of these printouts, but, in light of our desire to provide information to the Committee promptly, we have not had the opportunity to review systematically every name on the lists to ensure complete accuracy. Similarly, the Vice President's NSA office list was generated from NSA records; it is complete to the best of our knowledge, but again, we cannot attest to its absolute accuracy.

I hope the above information and attached materials are helpful to the Committee. I look forward to working with the Committee as its investigation proceeds. If you have any questions, please feel free to contact me at 456-6243.

Sincerely,



Michael X. Imbrosio
Associate Counsel to the President

cc: Michael W. Sheehy, Esq.

THE WHITE HOUSE
WASHINGTON

July 23, 1997

MEMORANDUM

TO: CHARLES F.C. RUFF
Counsel to the President

FROM: Michael X. Imbroscio *MD*
Associate Counsel to the President

RE: Draft Response to June 24, 1997 HPSCI Letter

JB -
Looks fine
to me, with
two edits.
Please review.
(Please save
for me.)

Attached please find a draft response to the June 24, 1997 letter to you from the HPSCI. I have spoken with the Deputy Counsel Chris Barton concerning the document request, and he confirmed that the Committee is seeking only broad policy documents relating to procedures in place for granting access to classified information. I had a general discussion about my understanding of the system in place, and we agreed that I would endeavor to provide him some information by the end of next week, August 1, 1997. The draft letter and attachments comprises the information I have gathered from the Security Office, the NSC, and the OVP.

I look forward to your comments as well as the comments of the below-noted interested persons. In particular, I ask all to inspect the employee lists to ensure accuracy and completeness to the extent possible. I note that we appear not to have caught certain OVP/NSA detailees.

I will be out of the office this Thursday, Friday, and next Monday, returning on Tuesday, July 29, 1997. I would appreciate if the recipients returned their respective drafts with comments to Brian Smith in OEOP Room 125 by close of business on Tuesday, July 29, 1997, so that the letter can be finalized.

Attachment

cc: Lanny A. Breuer
Don Goldberg
Elizabeth Brown
Alan J. Kreczko
James E. Baker
William H. Leary
Nelson Cunningham
Charles C. Easley

TAB A

Presidential Documents

Title 3—

Executive Order 12968 of August 2, 1995

The President

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, THEREFORE, 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 United States 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 U.S. 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 3 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 ac-

quired 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 sections 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 10 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 con-

tracting, 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 sections 2.6 and 3.3 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 applicant's 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 5 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 5 years and who have been retired or otherwise separated from United States Government employment for not more than 2 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. 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 the 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 subsection (b) of this section; 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's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection (a)(6) of this section.

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in subsection (a)(6) of this section 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 subsection (a) of this section. 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 subsection (a) of this section 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 subsection (a) of this section 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 Security Policy 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 is effective immediately.



THE WHITE HOUSE,
August 2, 1995.

TAB B

Withdrawal/Redaction Marker

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. paper	Security Procedures for the EOP Security Office. (23 pages)	11/1996	b(7)(E), b(7)(F)

COLLECTION:

Clinton Presidential Records
National Security Council
Staff Director (Nancy Soderberg)
OA/Box Number: 1421B

FOLDER TITLE:

[HSPCI Document Request re: WH Security Clearances, 1997] [1]

2006-1066-F

vz884

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]