Case Number: 2006-1066-F

FOIA MARKER

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

Folder Title:
Security Issues [1]

Staff Office-Individual:
Counsel's Office-Cerf, Christopher

Original OA/ID Number:
CF 432

Row:	Section:	Shelf:	Position:	Stack:
19	2	6	2	V

Withdrawal/Redaction Sheet
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. form	Procedures for Obtaining Building Passes for New Employees. (4 pages)	03/21/1994	b(7)(E)

COLLECTION:
Clinton Presidential Records
Counsel Office

OA/Box Number: CF 432

FOLDER TITLE:
Security Issues [1]

2006-1066-F
vz3552

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]

TO: Dawn Fen
Trey Sch

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF ADMINISTRATION
Washington, D.C. 20503

April 4, 1995

The Honorable
Richard C. Shelby
United States Senate
509 Hart Senate Office Building
Washington, D. C. 20510-0103

Dear Senator Shelby,

Since my testimony of Monday, March 27, 1995, I have reviewed the status of the individual random drug testing program. Currently, there are fifteen EOP employees who are the subject of an individualized random drug testing program. That figure, of course, may fluctuate in either direction as employees come and go. For example, five individuals who had participated in such a program are no longer here. By any measure, however, this figure constitutes a very small percentage of the total number of authorized EOP employees, which currently stands at 1,755.

As the existence of the special drug testing program itself demonstrates, this Administration is second to none in its commitment to maintain a drug free workplace. Every member of the White House staff is drug tested as a condition of his or her initial employment. In addition, all White House staff are subject to random drug testing. The special testing program is a precaution we take <u>above and beyond</u> these mandatory procedures. It applies only to a very limited pool of individuals whose drug use prior to joining the Administration, in the judgment of the Secret Service, warrants these additional measures. Needless to say, none of the individuals who are subject to such a program has ever tested positive.

Sincerely,

Patsy Thomasson

Patsy Thomasson
Special Assistant to the President
for Management and Administration
Director of the Office of Administration

COMPARISON QUESTIONS

We wish to obtain comments on the significance and/or causes of the following comparison results. Instances where you have responded to our questions regarding individual records that relate to specific comparisons are noted. Bracketed [] items are averages and numbers reflecting White House suggested deletions.

1-Comparing the date of appointment and the date of the drug test.

a. During 1993, people on average took their drug test 40 [29] days after EOD, whereas in 1994 people on average took their drug test 49 [12] days before EOD (e.g., WHO 110, WHO 337, WHO 338, WHO 354, WHO 375, and WHO 442).

b. During the entire period, WHO staff on average took their drug test 16 [27] days after EOD and OPD staff took 27 [25] days after EOD, whereas ONDCP and OA staff took their drug tests 73 [30] days before EOD on average.

2-Comparing the date of appointment and the date the SF-86 was signed.

a. Regarding this interval:

--36 [35] people took over 300 days to sign their SF-86s after EOD (e.g., WHO 66, WHO 110, WHO 251, and WHO 270),
--74 [72] people took between 201 and 300 days,
--80 [77] took between 101 and 200 days,
--306 [286] took between 0 and 100 days,
--87 [79] people signed their SF-86s between 1 and 100 days before EOD,
--16 [9] took between 101 and 300 days before EOD,
--5 [1] between 301 and 500 days before EOD (e.g., WHO 333), and
--9 [0] took over 500 days before EOD.

b. During the first quarter of 1993, staff took 121 [122] days on average to sign their SF-86 after EOD. During the second and third quarters of 1994, staff on average signed their SF-86 64 [3] days prior to EOD.

c. During the entire period, WHO staff took 87 [101] days on average to sign their SF-86 after EOD, and OPD staff took 68 [70] days. ONDCP and OA staff on average signed their SF-86s 77 days prior to EOD [13 days after EOD].

3-Comparing the date of appointment and the date the temporary pass was issued.

a. During the entire period, WHO and OPD staff on average received their temporary passes 7 [21] days after EOD, whereas contractors and ONDCP staff took 50 [58] days after EOD. OA and OVP staff on average received their temporary passes 34 days prior to EOD [7 days after EOD].

b. It took 36 [34] people over 100 days to receive a temporary pass after EOD (e.g., WHO 212) and 46 [42] people took between 51 and 100 days. There were 95 [56] people who received temporary passes an average of 122 [51] days prior to EOD.

4-Comparing the date of appointment and the date the permanent pass was issued.

a. The average has decreased from 388 [390] days in the first quarter of 1993 to 74 [116] days in the second and third quarters of 1994.

b. During the entire period, WHO, OPD, and OVP staff took 300 [319] days or more on average to receive a permanent pass after EOD, whereas ONDCP and OA staff took an average of 141 [192] days.

c. Regarding this interval:

--28 [27] people took over 500 days to go from EOD to the permanent pass issue date,
--123 [122] people took between 401 and 500 days,
--100 [97] people took between 301 and 400 days,
--119 [111] people took between 201 and 300 days,
--124 [101] people took between 0 and 200 days, and
--10 [0] people received permanent passes prior to EOD.

d. Of 504 [458] total permanent passes issued, only two [0] were issued prior to September 20, 1993.

5-Comparing the date of the drug test and the date the temporary pass was issued.

a. There were 289 [259] out of 570 [523] (50.7 [49.5] percent) who received temporary passes before getting drug tested. {May have answer.}

b. During the entire period, WHO, OPD, and OVP staff on average got their temporary passes 11 [6] days before they were drug tested, whereas ONDCP and OA staff were drug tested an average of 69 [71] days before getting their pass.

6-Comparing the date of the drug test and the date the FBI initiated its investigation.

a. There were 82 [67] people who had not been drug tested prior to the start of the FBI's investigation.

7-Comparing the date of the drug test and the date the FBI concluded its investigation.

a. There were 39 [29] people who had not been drug tested prior to the conclusion of the FBI's investigation.

8-Comparing the date the SF-86 was signed and the date the temporary pass was issued.

a. In 1993, 310 [289] people out of 450 [411] (68.9 [70.3] percent) received a temporary pass prior to signing an SF-86, whereas in 1994, this was true for 55 [45] of 158 [144] people (34.8 [31.3] percent).

b. During the entire period, WHO, OPD, and OVP staff on average received temporary passes prior to signing an SF-86. ONDCP and contractor staff on average signed the SF-86 prior to receiving a temporary pass.

9-Comparing the date the SF-86 was signed and the date the FBI initiated its investigation.

a. During the first half of 1993, it took 50 [48] days on average to go from the SF-86 signature date to the start of the FBI investigation. During 1994, it took 18 [18] days.

b. Regarding this interval:

--for 11 [9] people (e.g., WHO 168), the start of the FBI investigation was more than 200 days from the SF-86 signature date,
--for 26 [22] people it was between 101 and 200 days (e.g., OVP 3), and
--for 74 [67] it was between 51 and 100 days.

c. During the entire period, OVP staff took 84 [80] days on average to go from the SF-86 signature date to the start of the FBI investigation, more than twice as long as the overall average.

10-Comparing the date the temporary pass was issued and the date the FBI initiated its investigation.

a. During the first half of 1993, it took 132 [132] days on average to go from temporary pass issuance to the start of the FBI investigation. During 1994, the FBI investigation started 21 [6] days on average before the temporary pass was issued.

b. Regarding this interval:

--36 [32] people took over 300 days to go from temporary pass issuance to the start of the FBI investigation,
--88 [79] took between 201 and 300 days,
--108 [99] took between 101 and 200 days, and
--17 [12] people had FBI investigations start more than 100

days prior to receiving a temporary pass.

c. During the entire period, it took WHO and OVP staff 112 [112] days on average to go from temporary pass issuance to the start of the FBI investigation and it took contractors 3 [12] days. ONDCP staff on average had their investigations started before they got temporary passes.

11-Comparing the date the temporary pass was issued and the date the permanent pass was issued.

a. The average for the first quarter 1993 was 373 [374] days, whereas the average for the third quarter 1994 was 74 [83] days.

b. During the entire period, the average for WHO, OPD, and OVP was 313 [313] days, whereas the average for ONDCP, OA, and contractors was 172 [172] days.

12-Comparing the date the temporary pass was issued and the date of separation.

a. There were 4 [3] people who received temporary passes after they separated (e.g., WHO 75).

13-Comparing the date the FBI initiated its investigation and the date the FBI concluded its investigation.

a. During the first three quarters of 1993, it took 51 [51] days on average for the FBI to conduct its investigation. In 1994, the average was 70 [71] days. {May refer to the FBI.}

b. The FBI took over 100 days to conduct investigations on 37 [34] people (e.g., OA 10 and WHO 409). {May refer to the FBI.}

14-Comparing the date the FBI concluded its investigation and the date the permanent pass was approved.

a. Adjudication took:

--250 [249] days on average during the first half of 1993,
--123 [123] days on average during the last half of 1993, and
--46 [48] days on average during 1994.

b. Regarding this interval:

--16 [13] people took over 400 days to have their case adjudicated (e.g., WHO 41, WHO 312, and WHO 338),
--41 [36] people took between 301 and 400 days (e.g., WHO 213), and
--52 [49] people took between 201 and 300 days.

15-Comparing the date the permanent pass was approved and the date a permanent pass was issued.

a. This comparison averaged:

--30 [31] days during the last half of 1993,
--7 [8] days during the first half of 1994, and
--4 [4] days during the last half of 1994. {May refer to the Secret Service.}

b. It took 6 [6] people over 100 days to have their pass issued after it was approved (e.g., OVP 3). {May refer to the Secret Service.}

c. During the entire period, OVP staff took 37 [40] days on average to go from permanent pass approval to permanent pass issuance, three times longer than the overall average.

United States General Accounting Office

GAO Fax Transmittal Sheet

To: (Name and Address)

Chris Cerf

Telephone No. 456-2144 Fax Telephone No. 456-2146 Date ~~5-8~~ 5-10

From: (Name and Address)

David Hand

Telephone No. 512-4170 Fax Telephone No. 512-8786 Date

Subject:

Comparison Questions - Version 2

Additional Information

Acknowledgement Requested

1. ☐ Yes ☑ No
2. 6 pages, including this cover sheet, are being transmitted.
3. If pages are not received, call David Hand.

File: Farrell Letter

THE WHITE HOUSE

WASHINGTON

May 17, 1995

Thomas F. Farrell
Special Agent in Charge
U.S. Secret Service
White House Division
Room 14 Old Executive Office Building
Washington, D.C. 20500

Dear Mr. Farrell,

In light of a recent inquiry, I thought it would be useful to restate our views about the White House Personnel Security Office (WHPS). The WHPS is a division of the White House Counsel's Office. As Counsel to the President, I am ultimately responsible for its operation. Historically, however, the management and operation of the office has been delegated to one of the Associate Counsels. At present, I have charged Chris Cerf with that responsibility. The USSS should work with him on any issues of mutual interest to our respective offices.

Thank you very much.

Abner J. Mikva
Abner J Mikva
Counsel to the President

File: Security
Procedures

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. form	Procedures for Obtaining Building Passes for New Employees. (4 pages)	03/21/1994	b(7)(E)

COLLECTION:
Clinton Presidential Records
Counsel Office

OA/Box Number: CF 432

FOLDER TITLE:
Security Issues [1]

2006-1066-F
vz3552

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]

Copies Nelson
C did not
take w/ him
6/20/96

THE WHITE HOUSE

WASHINGTON

PERSONNEL INTERVIEWED

White House Office
- Mari Anderson, Executive Asst. to WH Per. Sec. Dir.
- Larry W. Croce, Military Office Security Director
- Craig Livingstone, Personnel Security Director
- Beth Nolan, Associate Council to the President
- John D. Podesta, Asst. to the President/Staff Secretary
- Claude A. Taylor, Director of Volunteers
- Paul A. Toback, Special Asst. to Chief of Staff
- Rod Von Lipsey, WH Fellow/Special Asst. to Chief of Staff
- Sharon E. Wagner, Admin. Asst. to the Staff Secretary
- Francis R. Wessel, Admin. Asst. to the Staff Secretary

National Security Council
- James E. Baker, Deputy Legal Advisor
- John W. Ficklin, Deputy Director Records Management
- Christopher L. George, Staff Information Assistant
- David E. Herrington, Adm. Office Systems Director
- Andrew S. Kerr, Staff Information Assistant
- Robert J. Manzanares, Adminstrative Office Director
- Patricia C. Nelson, Security Officer
- John W. Peggins, Systems Manager
- Ralph H. Sigler, Deputy Director WH Situation Room
- David S. Vantassel, Asst. Director Information Disclosure

National Economic Council
- Robert D. Kyle, Special Asst. to the President
- Elaine M. Mitsler, Executive Asst.-International Group

Office of the Vice President
- Todd J. Campbell, Counsel and Dir. of Adm. for the VP
- Joanne M. Hilty, Security Officer for the OVP

Council of Economic Advisors
- Elizabeth A. Kaminski, Admin. Officer and Security Coord.

Office of Administration
- Mary Coutts Beck, Director of Personnel Management
- Christopher D. Cerf, General Council
- Alejandro L. De Leyos, Mailroom Supervisor
- Charles C. Easley, Security Officer
- Mark E. Frownfelder, Security Specialist
- Lawrence R. Jurcich, Telecommunications and Security
- James L. MacDonald, Director Info. Systems and Technology
- Gwendolyn N. Weaver, Dep.Asst. Director for Info. Management

THE WHITE HOUSE

WASHINGTON

Office of Management and Budget
Roberta L. Foster, Secretary-National Security CCCI
Darrell A. Johnson, Deputy Asst. Director of Administration
Marilyn E. Jones, Secretary-Dep. Assoc. Dir. National Sec.
Anthony B. Wu, Budget Examiner/Acting Branch Chief CCCI

Office of National Drug Control Policy
Tilman Dean, Support Services Spec./Security Coordinator
Henry H. Marsden, Director Supply Reduction

Office of Science and Technology Policy
Barbara A. Ferguson, Administrative Office/Security Coord.
Deborah J. McGovern, Administrative Assistant
Joann Ward, Administrative Operations Assistant

President's Foreign Intelligence Advisory Board
Gwendolyn S. Watson, Administrative Officer/Security Coord.
Sandra E. Van Namee, Administrative Assistant

United States Trade Representative
Michael Arbogast, Systems Analyst
Lorraine Green, Human Resources Manager
Catherine A. Hofgren, Sup. Servs. Supervisor/Security Coord.
David Spetrino, Special Asst. to the USTR
Joan C. Steyaert, Director Computer Operations

White House Communications Agency
Francis Bartol, Communications Center
Paul Connelly, Security Officer
Robert Gutjahr, Deputy Security Officer
Lawrence Ledbetter, Communications Center

United States Secret Service
Arnie Cole, WH Sec. Branch-Investigations/Access Controls
Lt. Ron Elie, WH Uniformed Division
Tom Farrell, WH Security Branch Chief
Capt. Flanagen, WH Uniformed Division
Capt. J.J. Hampton, WH Uniformed Division
Officer Richard Tozier, WH Uniformed Division
Don Flynn, WH Security Branch
John J. Robey, Technical Services Branch Chief

General Services Administration
Lawrence Downes, Shredder Room NEOB

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN ______________________ AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and *952, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

(Continue on reverse.)

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)

WITNESS

THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.

SIGNATURE	DATE

NAME AND ADDRESS (Type or print)

ACCEPTANCE

THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.

SIGNATURE	DATE

NAME AND ADDRESS (Type or print)

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

DRAFT

SENSITIVE BUT UNCLASSIFIED

TO: Mr. Christopher D. Cerf
General Counsel
Office of Administration
Executive Office of the President

May 27, 1994

FROM: Christopher M.B. Disney
John R. Hancock
Bureau of Diplomatic Security
US Department of State

SUBJ: Review of EOP Security Issues

The Bureau of Diplomatic Security of the Department of State was informally requested to assist the Executive Office of the President in conducting a review of procedures involving the handling and storage of national security information. The review was conducted during the period May 16-27, 1994, by the reporting officers who were detailed to the EOP for the duration of the review.

The review was necessarily limited in scope due to time restrictions but, in all, 62 interviews were conducted as shown on the attached listing of personnel. In addition to interviewing EOP personnel, including detailees, an after hours review of USSS-UD security check procedures was conducted. Documentation reviewed included items such as the White House Staff Manual, OPM instructions and a variety of EOP security-related memoranda.

It is the opinion of reporting officers that, in general, procedures governing the handling of national security information ranged from highly effective to those requiring improvement. Certain EOP elements such as the NSC, WHMO, ONDCP, PFIAB and others which handle large quantities of classified information appeared to have viable, pro-active and aggressive security programs. Procedures reviewed within these elements adhere to USG regulations and commonly accepted practice. Officers charged with security responsibilities are well versed in procedure and provided

DRAFT

evidence of well-structured, detailed and thorough programs. All personnel interviewed displayed extremely positive attitudes towards the conduct of the review and voiced the expected commitment towards the protection of classified and sensitive information.

Areas requiring improvement and modification of procedure are addressed in the attached outline. We found that only certain security practices and procedures generally involving offices not handling large quantities of classified information needed attention. Corrective action, in most cases, could be achieved by an aggressive security awareness training program and revision of some procedures. In addition, the recommended consolidation of security functions would provide a comprehensive, uniform and centrally-managed approach with clear lines of authority and responsibility.

The issues addressed and recommendations which resulted are divided into four general areas: (1) Procedural Security, (2) Personnel Security, (3) Security Awareness and (4) Security Organization.

DRAFT

1. <u>Procedural Security</u>

a. Protection of national security information was the major purpose of this review. Most EOP elements indicated their handling of classified information was minimal. Examination disclosed procedures which ranged from highly effective to those requiring improvement.

A common set of procedures addressing the accessing, handling and disposal of classified information does not exist. Procedures have been issued by the EOP Security Officer within the Office of Administration for certain EOP offices but they are dated (June 1988) and have not been established for or applied to all elements of the EOP. Several organizations within the EOP x appear to lack formal procedures x for governing the access and handling of national security information.

Recommendation No. 1
Uniform procedures based upon existing USG regulations should be drafted and promulgated to all entities which comprise the Executive Office of the President.

b. Classified information enters EOP elements either electronically (classified communications circuits or secure fax) or hand-carried by courier. In each of the entities of the EOP structure, material is ordinarily distributed from a central distribution point or is received through a terminal in a SCIF. Highly sensitive material, for example the NID, appears for the most part to receive the requisite handling and protection with the exception that in some cases the NID is not returned in a timely manner causing extensive administrative problems in conducting the necessary tracking procedure. In one case, the NID had not been returned for almost six months. In another case, the NID was routinely included in a comprehensive daily briefing book and given to a secretary for further distribution. This person is not, as of the date of this report, cleared for access to SCI.

Recommendation No. 2
All recipients of the NID and other numerically controlled documents should be reminded by memorandum from as high a level as appropriate of their obligation to restrict access to this material and return these documents to the issuing office within the prescribed time period. In addition, strict adherence must be maintained to the limitations placed upon distribution of the NID by the CIA. Access by personnel not on the distribution list must be approved by the originating office within CIA.

c. Within the EOP, outside the NSC, WHMO, PFIAB, ONDCP and a few other exceptions, there appears to be remarkably little national security information processed and stored. There is, however, a significant amount of information which is extremely sensitive in nature -- the President's Daily Schedule is one example. Anecdotally, during reporting officers' assignment to the OEOB, part of the time was spent in Room 502. Each morning a copy of the President's Schedule for that day and, on one occasion, a 3-month advance schedule was found in an envelope in front of Room 502 marked for "Jeff Watson" who presumably formerly occupied the office. The Schedule was unclassified and uncontrolled in an unsealed envelope.

Recommendation No. 3
Procedures for limiting distribution and enhancing protection of sensitive information, especially the President's Daily Schedule, should be reviewed and improvements made as appropriate. This process should also extend to information transmitted by unclas fax between the White House Complex and Presidential trip site locations.

d. Personnel interviewed were aware and acknowledged that the EOP/OA computer system in use (OASIS), was restricted to unclassified information. However, if secure systems did not exist in their office space, not all personnel were aware how classified information could be processed. It is noted that the IST Division of OA has recently completed

a draft directive on InfoSec concerns. It appears thorough, detailed and broad in scope and should be promulgated as soon as possible.

Recommendation No. 4
Procedures should be issued reinforcing the requirement not to process classified information on non-secure systems. Personnel should also be made aware of available automated systems which can be utilized for processing classified information and the highest level of information permitted.

e. Procedures for disposition of classifed material in many office areas seemed unclear. Cursory reviews of many office spaces detected unusually few ~~classified~~ SECURITY containers.

Recommendation No. 5
A thorough survey should be conducted by each agency/office security officer to determine the exact requirement for security containers with an emphasis on reducing any classified holdings to the greatest extent possible but insuring that the remainder receive appropriate storage in approved containers. In addition, combinations on all ~~classified~~ security containers should be changed upon the departure of the office incumbent and/or at least once a year. Records should be maintained. It may be beneficial to have one or more common security containers located in the West Wing first and second floor areas where classified can be stored as required. It is also noted that SCIFs are not established on these two floors. All SCI material must, therefore, be secured in the Sit Room on the ground floor.

f. Few offices are equipped with shredders; most rely on burn bags. Discussions with a variety of employees revealed an inconsistent approach to the burn bag process. Some were collected by USSS-UD and others were delivered to a central shredding facility. Some employees seemed unsure of the process and used burn bags for disposal of unclassified material. Anecdotally, reporting officers discovered an unsecured burn bag in an unoccupied office in the OEOB at OOB on a Monday

morning. It was not checked for classified material. It had been unprotected for an unknown period over a week-end.

Recommendation No. 6
Clear, consistent procedures should be established for the collection/disposal of classified waste material. Ensure "open storage" is not permitted in unauthorized spaces. Each office which processes/handles classified information should utilize a standardized COB check list. After hours checks by USSS-UD should include checking for unsecured burn bags, classified information left unprotected and open containers.

Recommendation No. 7
Instructions issued on May 16, 1994 (attached) by Ms. Patsy Thomasson should be enforced. The shredder operator at the NEOB complained that burn bags continue to be piled in front of his door at OOB each morning. Each would have been unprotected on an unsecure loading dock area for varying periods and therefore subject to compromise.

g. Hard copy material is hand-carried throughout the EOP complex which includes the NEOB, the OEOB, the Winder Building, ONDCP and the White House. Procedures lack uniformity and vary in the degree of protection afforded. The EOP Mail Room process (Red Tag) appears effective but personnel from many offices also individually hand deliver material.

Recommendation No. 8
Instructions should be issued clarifying courier procedures and lockable courier pouches should be issued to central offices within each building for the transport of SCI material. Personnel transporting classified/sensitive information outside the OEOB/WH complex should be reminded of requirements and procedures.

Recommendation No. 9
Storage/access procedures for SCI and other codeword material should be thoroughly examined especially in West Wing offices. A walk-through by reporting officers at 2300 hours on 5/25 disclosed the fact that (a) few,

if any, safes are available in West Wing working spaces, and (b) at COB, within certain West Wing first floor offices, material was simply left on the desk - a TS document was discovered unprotected on one desk. It is noted, however, that a UD officer is present in front of the Oval Office 24 hours a day making the possibility of compromise remote. Due to the quantity of documents seen unprotected in various offices, the presence of other collateral or code word material cannot be discounted.

Recommendation No. 10
New COB procedures should be established for certain first floor West Wing offices. After departure of the principal, staff members should be required to collect all classified/sensitive material and secure it. Safes should be procured for this purpose. While access to the West Wing is controlled by UD personnel and chars are escorted (ratio unknown), material left exposed could be subjected to scrutiny by char force or other uncleared personnel perhaps being escorted on tours.

Recommendation No. 11
Certain offices have evening secretarial shifts. If the secretary leaves prior to collection of the burn bag by the UD officer, she simply leaves the unsecured bag in full view. This procedure is also employed by day shift personnel. Burn bags should receive more positive control. One option would be for staff members to hand carry the closed burn bag to a central holding room for later collection by UD. This will insure positive control from the time a document enters the office to its destruction.

Recommendation No. 12
Within the EOP, burn bag destruction procedures fall into two general categories: (1) NSC (both Sit Room and OEOB) material is held in a secure area for weekly collection and destruction by CIA courier, and (2) Collection by UD personnel and office staff and carriage to one of two destruction facilities in the OEOB (Basement Area) or NEOB (Loading Dock). In the latter category, material is taken out of the burn bag and placed on the conveyor belt which carries it to the shredder. At that point the material is in full view of the operator. SCI material may be present and operators have not been authorized SCI access. Either operators should be

SCI accessed or instructions should be promulgated to staff to segregate SCI from collateral waste.

2. Personnel Security

a. Within the White House Personnel Security Office (WHPS), a 17-step process has been established (attached) which results in the issuance of a building pass. In addition, under the signature of the Chief of Staff, an instruction was issued on March 14, 1994 (attached) concerning completion of security related paperwork for new employees. Procedures seem clear, are endorsed by senior management and provide for punitive measures for non-compliance. The areas which may warrant additional attention, however, are the adjudication process and the timeliness of the entire procedure. The FBI conducts a SSBI and returns the ROI to the WHPS where it is reviewed for issues of suitability and potential embarrassment to the Administration. The report is then forwarded to the USSS for review from a protective intelligence perspective and a permanent pass issued as appropriate.

The pass that is issued appears to be adjudicated primarily on the basis of suitability and potential threat to the President. While not dissimilar, adjudicative criteria for access to national security information which would include potential CI concerns does not appear to be specifically addressed in this process. Issuance of the pass, however, is in fact viewed as the potential for authority to access classified information up to and including Top Secret. There is some confusion as to exactly what issuance of a permanent pass means.

Recommendation No. 1
The system employed by the various elements of the EOP to issue building passes and to grant clearances lacks uniformity. While unique requirements exist, for example, within the WHO and WHMO, procedures should be as common as possible. A Task Force composed of EOP Security and Personnel Officers should address this issue and arrive at consensus.

Redundant areas should be identified and avoided. N.B. During the course of the review, several comments were made regarding the excessive length of the clearance process which caused administrative problems. It is noted, however, that a great deal of attention has been given to this issue and as of May 11th, 76.~~52~~% of the staff had been issued passes. The balance were either in the adjudication process, pending a BI or awaiting paperwork (2.~~83~~%).

Recommendation No. 2
If, in the adjudication process, a conscious application of criteria governing access to national security information is not applied, then this should occur forthwith. Personnel involved in the adjudication process should refamiliarize themselves with these instructions which are included in Chapters 731, 732, 735 and 736 of the Federal Personnel Manual as amended by the FPM Sunset Document.

Note: The Diplomatic Security Service is prepared to detail a senior Personnel Security Adjudicator to work within the WHPS for a short period to assist in the establishment of this process and provide informal OJT of personnel as necessary.

Recommendation No. 3
To assist in the timely retrieval of information concerning the level of clearance granted/held by each employee who is a member of any element of the EOP or who holds any type of pass allowing unescorted access to any EOP facility, a data base should be created. Information should be available in this system to any of the security officers within the EOP structure. This will also aid considerably in the passing of clearances in a timely fashion to other USG agencies.

Recommendation No. 4
Signing of the SF 312 and the resulting acknowledgement of one's responsibilities in the protection of classified information is inconsistent. Throughout the EOP, common procedures should be established in the clearance issuance and briefing process to insure the SF 312 is signed by each person granted access to classified material.

Recommendation No. 5
The building pass system seemed unnecessarily complicated with a somewhat bewildering array of variously colored and lettered passes. The brevity of this survey did not permit a detailed analysis of the system but it is recommended that this issue be another agenda item for the EOP Security ~~Officer~~ Coordinator group to address.

Recommendation No. 6
Employment of Volunteers and Interns in areas in which classified material is handled should be severely limited. If unavoidable, those so employed should be cleared up to the Secret level with access limited to that level. This can be accomplished through conduct of ~~a~~ NACI.

Recommendation No. 7
The wording of the memorandum from WHPS regarding the completion of a favorable BI and the authorization for a permanent building pass and security clearance should be revised. It is imprecise and is not understood by at least one EOP unit security officer.

Recommendation No. 8
WHPS personnel are under pressure to insure that personnel are cleared in as short a time frame as possible. Given the functions expected of this office, it appears extremely understaffed and in unusually cramped physical space. Efforts to alleviate both problems should be undertaken as soon as possible.

Recommendation No 9
The WHPS staff is required to adjudicate a wide variety and a vast number of background investigations. The process ultimately allows access to national security information. All EOP personnel, especially those in the WHPS, who are charged with adjudicative responsibility should receive formalized training. It is recommended that this occur to insure proper criteria is applied and to maintain the credibility of the process.

4 Recommendation No. 10
It is recommended that a program be initiated as soon as possible to subject each file on the pending clearance/building pass list to a thorough review to ascertain precise disposition. It is suggested that the process begin with the WHO, the most highly visible office within the EOP.

Recommendation No. 11
It is recommended that a survey be conducted beginning with WHO staff to determine who, in fact, has access to collateral and SCI material. Commensurate levels of clearance and access should be effected and a central record maintained.

Recommendation No. 12
The "White House Office Supplemental Information Sheet for Personnel Action" should be slightly revised as shown in attachment. Inclusion of this information should help speed the process of accessing classified information since Secret/Confidential access can be granted by satisfactory completion of a NACI pending completion of the full field BI.

3. Security Awareness

a. Some procedures are in effect for certain security related issues. For example, page B-6 of the White House Staff Manual outlines how unsecured classified material is to be handled. However, it seemed clear that procedures are neither widely known nor strictly followed. The Security Awareness program should be so designed as to (1) Initially brief incoming personnel, (2) periodically remind employees of their security related responsibilities and (3) brief employees on unique security and CI concerns prior to travel abroad. During the course of this review, several persons commented that "security problems" were most evident in areas populated by "political appointees" as opposed to career civil service/detailed personnel. Most agreed that security awareness training was sorely needed. It was noted, for example, that WHCA offered two

separate briefings on overseas security issues with one person showing up for the first and only a handful for the second. It is also noted that the Security Office, OA, is engaged in a periodic training effort.

X Recommendation No. 1
A system-wide program of security training should be initiated. It is suggested that this include briefings to junior and mid-level staff and a comprehensive series of periodic memoranda to senior staff. Emphasis should be placed on the handling and disposal of classified material, classification management and the unique nature of employment within the EOP which may make personnel particularly attractive to Hostile Intelligence Services (HOIS).

Recommendation No. 2
To assist the EOP Security Staff in the conduct of a security awareness program, the Diplomatic Security Service is prepared to present a 45-minute briefing program with Q&As addressing two primary areas: (a) Handling of national security information and (b) Technical security concerns. The latter is designed to demonstrate vulnerabilities of such areas as telephone usage, particularly the ease in interception of conversations on cellular phones.

Recommendation No. 3
The existing 37 minute security awareness instructional tape should be re-done. It is too long, attempts to cover too many unrelated issues and tends to lose the attention of those viewing. It needs to be shortened to a maximum of 15 minutes and considerably tightened in scope and presentation. It should be accompanied by a presentation by each agency security officer addressing agency-specific security issues. It is noted that this effort has been initiated by the OA Security Officer.

Recommendation No. 4
An EOP Security Handbook should be developed and distributed to all current and new personnel. It should include information presented in the tape, contact numbers for security personnel, emergency numbers,

description of procedures and other related information. It is noted that the Security Office, OVP, has developed and issued a detailed and extremely useful document which could provide the basis for an EOP Handbook.

4. Security Organization

a. Virtually every agency within the EOP has its own security coordinator but the entire system is fragmented and lacks cohesion and uniformity. Security procedures vary extensively with minimal cross pollination despite periodic meeting of the Security Coordinators group. There is little back-up and when individuals are on travel status procedures slow down and often stop. Uniformity is achieved only on an informal, ad hoc basis. Under a centralized, properly staffed security directorate, policy
would be uniform and procedures appropriately enforced.

Recommendation No. 1
To facilitate a comprehensive, EOP-wide security program, it is suggested that the existing fragmented operation ~~should~~ be overhauled. For the recommendations made herein to be effective, a change must be made in the way the security program is managed. Therefore, a position should be created to coordinate the wide array of EOP security programs. The primary function would be to establish uniform policy and procedures for all elements within the EOP structure. The incumbent should be a security professional (career or detailed) and be the senior security officer within the EOP. The position could be possibly entitled Director of Security, Executive Office of the President, with all existing Security Coordinators reporting to him/her for security programming purposes only. He/She should report to as high a level as possible within the General Counsel, WHO, which will add authority to the function.

Note: To assist EOP Staff in implementing this recommendation, the Diplomatic Security Service is prepared to detail a senior officer to provide guidance and direction as required in establishing such a position.

Attachments: As stated

THE WHITE HOUSE

WASHINGTON

PERSONNEL INTERVIEWED

White House Office
- Mari Anderson, Executive Asst. to WH Per. Sec. Dir.
- Larry W. Croce, Military Office Security Director
- Craig Livingstone, Personnel Security Director
- Beth Nolan, Associate Council to the President
- John D. Podesta, Asst. to the President/Staff Secretary
- Claude A. Taylor, Director of Volunteers
- Paul A. Toback, Special Asst. to Chief of Staff
- Rod Von Lipsey, WH Fellow/Special Asst. to Chief of Staff
- Sharon E. Wagner, Admin. Asst. to the Staff Secretary
- Francis R. Wessel, Admin. Asst. to the Staff Secretary

National Security Council
- James E. Baker, Deputy Legal Advisor
- John W. Ficklin, Deputy Director Records Management
- Christopher L. George, Staff Information Assistant
- David E. Herrington, Adm. Office Systems Director
- Andrew S. Kerr, Staff Information Assistant
- Robert J. Manzanares, Adminstrative Office Director
- Patricia C. Nelson, Security Officer
- John W. Peggins, Systems Manager
- Ralph H. Sigler, Deputy Director WH Situation Room
- David S. Vantassel, Asst. Director Information Disclosure

National Economic Council
- Robert D. Kyle, Special Asst. to the President
- Elaine M. Mitsler, Executive Asst.-International Group

Office of the Vice President
- Todd J. Campbell, Counsel and Dir. of Adm. for the VP
- Joanne M. Hilty, Security Officer for the OVP

Council of Economic Advisors
- Elizabeth A. Kaminski, Admin. Officer and Security Coord.

Office of Administration
- Mary Coutts Beck, Director of Personnel Management
- Christopher D. Cerf, General Council
- Alejandro L. De Leyos, Mailroom Supervisor
- Charles C. Easley, Security Officer
- Mark E. Frownfelder, Security Specialist
- Lawrence R. Jurcich, Telecommunications and Security
- James L. MacDonald, Director Info. Systems and Technology
- Gwendolyn N. Weaver, Dep.Asst. Director for Info. Management

THE WHITE HOUSE

WASHINGTON

Office of Management and Budget
- Roberta L. Foster, Secretary-National Security CCCI
- Darrell A. Johnson, Deputy Asst. Director of Administration
- Marilyn E. Jones, Secretary-Dep. Assoc. Dir. National Sec.
- Anthony B. Wu, Budget Examiner/Acting Branch Chief CCCI

Office of National Drug Control Policy
- Tilman Dean, Support Services Spec./Security Coordinator
- Henry H. Marsden, Director Supply Reduction

Office of Science and Technology Policy
- Barbara A. Ferguson, Administrative Office/Security Coord.
- Deborah J. McGovern, Administrative Assistant
- Joann Ward, Administrative Operations Assistant

President's Foreign Intelligence Advisory Board
- Gwendolyn S. Watson, Administrative Officer/Security Coord.
- Sandra E. Van Namee, Administrative Assistant

United States Trade Representative
- Michael Arbogast, Systems Analyst
- Lorraine Green, Human Resources Manager
- Catherine A. Hofgren, Sup. Servs. Supervisor/Security Coord.
- David Spetrino, Special Asst. to the USTR
- Joan C. Steyaert, Director Computer Operations

White House Communications Agency
- Francis Bartol, Communications Center
- Paul Connelly, Security Officer
- Robert Gutjahr, Deputy Security Officer
- Lawrence Ledbetter, Communications Center

United States Secret Service
- Arnie Cole, WH Sec. Branch-Investigations/Access Controls
- Lt. Ron Elie, WH Uniformed Division
- Tom Farrell, WH Security Branch Chief
- Capt. Flanagen, WH Uniformed Division
- Capt. J.J. Hampton, WH Uniformed Division
- Officer Richard Tozier, WH Uniformed Division
- Don Flynn, WH Security Branch
- John J. Robey, Technical Services Branch Chief

General Services Administration
- Lawrence Downes, Shredder Room NEOB

SENSITIVE BUT UNCLASSIFIED

TO: Mr. Christopher D. Cerf
White House Counsel's Office
Executive Office of the President

May 27, 1994

FROM: Christopher M.B. Disney
John R. Hancock
Bureau of Diplomatic Security
US Department of State

SUBJ: Review of EOP Security Issues

The Bureau of Diplomatic Security of the Department of State was informally requested to assist the Executive Office of the President in conducting a review of procedures involving the handling and storage of national security information. The review was conducted during the period May 16-27, 1994, by the reporting officers who were detailed to the EOP for the duration of the review.

The review was necessarily limited in scope due to time restrictions but, in all, 62 interviews were conducted as shown on the attached listing of personnel. In addition to interviewing EOP personnel, including detailees, an after hours review of USSS-UD security check procedures was conducted. Documentation reviewed included items such as the White House Staff Manual, OPM instructions and a variety of EOP security-related memoranda.

It is the opinion of reporting officers that, in general, procedures governing the handling of national security information ranged from highly effective to those requiring improvement. Certain EOP elements such as the NSC, WHMO, ONDCP, PFIAB and others which handle large quantities of classified information appeared to have viable, pro-active and aggressive security programs. Procedures reviewed within these elements adhere to USG regulations and commonly accepted practice. Officers charged with security responsibilities are well versed in procedure and provided

evidence of well-structured, detailed and thorough programs. All personnel interviewed displayed extremely positive attitudes towards the conduct of the review and voiced the expected commitment towards the protection of classified and sensitive information.

Areas requiring improvement and modification of procedure are addressed in the attached outline. We found that only certain security practices and procedures generally involving offices not handling large quantities of classified information needed attention. Corrective action, in most cases, could be achieved by an aggressive security awareness training program and revision of some procedures. In addition, the recommended consolidation of security functions would provide a comprehensive, uniform and centrally-managed approach with clear lines of authority and responsibility.

The issues addressed and recommendations which resulted are divided into four general areas: (1) Procedural Security, (2) Personnel Security, (3) Security Awareness and (4) Security Organization.

1. <u>Procedural Security</u>

a. Protection of national security information was the major purpose of this review. Most EOP elements indicated their handling of classified information was minimal. Examination disclosed procedures which ranged from highly effective to those requiring improvement.

A common set of procedures addressing the accessing, handling and disposal of classified information does not exist. Procedures have been issued by the EOP Security Officer within the Office of Administration for certain EOP offices but they are dated (June 1988) and have not been established for or applied to all elements of the EOP. Several organizations within the EOP appear to lack formal procedures for governing the access and handling of national security information.

Recommendation No. 1
Uniform procedures based upon existing USG regulations should be drafted and promulgated to all entities which comprise the Executive Office of the President.

b. Classified information enters EOP elements either electronically (classified communications circuits or secure fax) or hand-carried by courier. In each of the entities of the EOP structure, material is ordinarily distributed from a central distribution point or is received through a terminal in a SCIF. Highly sensitive material, for example the NID, appears for the most part to receive the requisite handling and protection with the exception that in some cases the NID is not returned in a timely manner causing extensive administrative problems in conducting the necessary tracking procedure. In one case, the NID had not been returned for almost six months. In another case, the NID was routinely included in a comprehensive daily briefing book and given to a secretary for further distribution. This person is not, as of the date of this report, cleared for access to SCI.

Recommendation No. 2
All recipients of the NID and other numerically controlled documents should be reminded by memorandum from as high a level as appropriate of their obligation to restrict access to this material and return these documents to the issuing office within the prescribed time period. In addition, strict adherence must be maintained to the limitations placed upon distribution of the NID by the CIA. Access by personnel not on the distribution list must be approved by the originating office within CIA.

NSC

c. Within the EOP, outside the NSC, WHMO, PFIAB, ONDCP and a few other exceptions, there appears to be remarkably little national security information processed and stored. There is, however, a significant amount of information which is extremely sensitive in nature -- the President's Daily Schedule is one example. Anecdotally, during reporting officers' assignment to the OEOB, part of the time was spent in Room 502. Each morning a copy of the President's Schedule for that day and, on one occasion, a 3-month advance schedule was found in an envelope in front of Room 502 marked for "Jeff Watson" who presumably formerly occupied the office. The Schedule was unclassified and uncontrolled in an unsealed envelope.

Recommendation No. 3
Procedures for limiting distribution and enhancing protection of sensitive information, especially the President's Daily Schedule, should be reviewed and improvements made as appropriate. This process should also extend to information transmitted by unclas fax between the White House Complex and Presidential trip site locations.

d. Personnel interviewed were aware and acknowledged that the EOP/OA computer system in use (OASIS), was restricted to unclassified information. However, if secure systems did not exist in their office space, not all personnel were aware how classified information could be processed. It is noted that the IST Division of OA has recently completed

a draft directive on InfoSec concerns. It appears thorough, detailed and broad in scope and should be promulgated as soon as possible.

Recommendation No. 4
Procedures should be issued reinforcing the requirement not to process classified information on non-secure systems. Personnel should also be made aware of available automated systems which can be utilized for processing classified information and the highest level of information permitted.

e. Procedures for disposition of classifed material in many office areas seemed unclear. Cursory reviews of many office spaces detected unusually few security containers.

Recommendation No. 5
A thorough survey should be conducted by each agency/office security officer to determine the exact requirement for security containers with an emphasis on reducing any classified holdings to the greatest extent possible but insuring that the remainder receive appropriate storage in approved containers. In addition, combinations on all security containers should be changed upon the departure of the office incumbent and/or at least once a year. Records should be maintained. It may be beneficial to have one or more common security containers located in the West Wing first and second floor areas where classified can be stored as required. It is also noted that SCIFs are not established on these two floors. All SCI material must, therefore, be secured in the Sit Room on the ground floor.

f. Few offices are equipped with shredders; most rely on burn bags. Discussions with a variety of employees revealed an inconsistent approach to the burn bag process. Some were collected by USSS-UD and others were delivered to a central shredding facility. Some employees seemed unsure of the process and used burn bags for disposal of unclassified material. Anecdotally, reporting officers discovered an unsecured burn bag in an unoccupied office in the OEOB at OOB on a Monday

morning. It was not checked for classified material. It had been unprotected for an unknown period over a week-end.

Recommendation No. 6
Clear, consistent procedures should be established for the collection/disposal of classified waste material. Ensure "open storage" is not permitted in unauthorized spaces. Each office which processes/handles classified information should utilize a standardized COB check list. After hours checks by USSS-UD should include checking for unsecured burn bags, classified information left unprotected and open containers.

Recommendation No. 7
Instructions issued on May 16, 1994 by Ms. Patsy Thomasson should be enforced. The shredder operator at the NEOB complained that burn bags continue to be piled in front of his door at OOB each morning. Each would have been unprotected on an unsecure loading dock area for varying periods and therefore subject to compromise.

g. Hard copy material is hand-carried throughout the EOP complex which includes the NEOB, the OEOB, the Winder Building, ONDCP and the White House. Procedures lack uniformity and vary in the degree of protection afforded. The EOP Mail Room process (Red Tag) appears effective but personnel from many offices also individually hand deliver material.

Recommendation No. 8
Instructions should be issued clarifying courier procedures and lockable courier pouches should be issued to central offices within each building for the transport of SCI material. Personnel transporting classified/sensitive information outside the OEOB/WH complex should be reminded of requirements and procedures.

Recommendation No. 9
Storage/access procedures for SCI and other codeword material should be thoroughly examined especially in West Wing offices. A walk-through by reporting officers at 2300 hours on 5/25 disclosed the fact that (a) few,

if any, safes are available in West Wing working spaces, and (b) at COB, within certain West Wing first floor offices, material was simply left on the desk - a TS document was discovered unprotected on one desk. It is noted, however, that a UD officer is present in front of the Oval Office 24 hours a day making the possibility of compromise remote. Due to the quantity of documents seen unprotected in various offices, the presence of other collateral or code word material cannot be discounted.

Recommendation No. 10
New COB procedures should be established for certain first floor West Wing offices. After departure of the principal, staff members should be required to collect all classified/sensitive material and secure it. Safes should be procured for this purpose. While access to the West Wing is controlled by UD personnel and chars are escorted (ratio unknown), material left exposed could be subjected to scrutiny by char force or other uncleared personnel perhaps being escorted on tours.

Recommendation No. 11
Certain offices have evening secretarial shifts. If the secretary leaves prior to collection of the burn bag by the UD officer, she simply leaves the unsecured bag in full view. This procedure is also employed by day shift personnel. Burn bags should receive more positive control. One option would be for staff members to hand carry the closed burn bag to a central holding room for later collection by UD. This will insure positive control from the time a document enters the office to its destruction.

Recommendation No. 12
Within the EOP, burn bag destruction procedures fall into two general categories: (1) NSC (both Sit Room and OEOB) material is held in a secure area for weekly collection and destruction by CIA courier, and (2) Collection by UD personnel and office staff and carriage to one of two destruction facilities in the OEOB (Basement Area) or NEOB (Loading Dock). In the latter category, material is taken out of the burn bag and placed on the conveyor belt which carries it to the shredder. At that point the material is in full view of the operator. SCI material may be present and operators have not been authorized SCI access. Either operators should be

SCI accessed or instructions should be promulgated to staff to segregate SCI from collateral waste.

2. Personnel Security

a. Within the White House Personnel Security Office (WHPS), a 17-step process has been established which results in the issuance of a building pass. In addition, under the signature of the Chief of Staff, an instruction was issued on March 14, 1994 concerning completion of security related paperwork for new employees. Procedures seem clear, are endorsed by senior management and provide for punitive measures for non-compliance. The areas which may warrant additional attention, however, are the adjudication process and the timeliness of the entire procedure. The FBI conducts a SSBI and returns the ROI to the WHPS where it is reviewed for issues of suitability and potential embarrassment to the Administration. The report is then forwarded to the USSS for review from a protective intelligence perspective and a permanent pass issued as appropriate.

The pass that is issued appears to be adjudicated primarily on the basis of suitability and potential threat to the President. While not dissimilar, adjudicative criteria for access to national security information which would include potential CI concerns does not appear to be specifically addressed in this process. Issuance of the pass, however, is in fact viewed as the potential for authority to access classified information up to and including Top Secret. There is some confusion as to exactly what issuance of a permanent pass means.

Recommendation No. 1
The system employed by the various elements of the EOP to issue building passes and to grant clearances lacks uniformity. While unique requirements exist, for example, within the WHO and WHMO, procedures should be as common as possible. A Task Force composed of EOP Security and Personnel Officers should address this issue and arrive at consensus.

Redundant areas should be identified and avoided. N.B. During the course of the review, several comments were made regarding the excessive length of the clearance process which caused administrative problems. It is noted, however, that a great deal of attention has been given to this issue and as of May 11th, 76% of the staff had been issued passes. The balance were either in the adjudication process, pending a BI or awaiting paperwork (2%).

Recommendation No. 2
If, in the adjudication process, a conscious application of criteria governing access to national security information is not applied, then this should occur forthwith. Personnel involved in the adjudication process should refamiliarize themselves with these instructions which are included in Chapters 731, 732, 735 and 736 of the Federal Personnel Manual as amended by the FPM Sunset Document.

Note: The Diplomatic Security Service is prepared to detail a senior Personnel Security Adjudicator to work within the WHPS for a short period to assist in the establishment of this process and provide informal OJT of personnel as necessary.

Recommendation No. 3
To assist in the timely retrieval of information concerning the level of clearance granted/held by each employee who is a member of any element of the EOP or who holds any type of pass allowing unescorted access to any EOP facility, a data base should be created. Information should be available in this system to any of the security officers within the EOP structure. This will also aid considerably in the passing of clearances in a timely fashion to other USG agencies.

Recommendation No. 4
Signing of the SF 312 and the resulting acknowledgement of one's responsibilities in the protection of classified information is inconsistent. Throughout the EOP, common procedures should be established in the clearance issuance and briefing process to insure the SF 312 is signed by each person granted access to classified material.

Recommendation No. 5
The building pass system seemed unnecessarily complicated with a somewhat bewildering array of variously colored and lettered passes. The brevity of this survey did not permit a detailed analysis of the system but it is recommended that this issue be another agenda item for the EOP Security Coordinator group to address.

Recommendation No. 6
Employment of Volunteers and Interns in areas in which classified material is handled should be severely limited. If unavoidable, those so employed should be cleared up to the Secret level with access limited to that level. This can be accomplished through conduct of a NACI.

Recommendation No. 7
The wording of the memorandum from WHPS regarding the completion of a favorable BI and the authorization for a permanent building pass and security clearance should be revised. It is imprecise and is not understood by at least one EOP unit security officer.

Recommendation No. 8
WHPS personnel are under pressure to insure that personnel are cleared in as short a time frame as possible. Given the functions expected of this office, it appears extremely understaffed and in unusually cramped physical space. Efforts to alleviate both problems should be undertaken as soon as possible.

Recommendation No 9
The WHPS staff is required to adjudicate a wide variety and a vast number of background investigations. The process ultimately allows access to national security information. All EOP personnel, especially those in the WHPS, who are charged with adjudicative responsibility should receive formalized training. It is recommended that this occur to insure proper criteria is applied and to maintain the credibility of the process.

Recommendation No. 10
It is recommended that a program be initiated as soon as possible to subject each file on the pending clearance/building pass list to a thorough review to ascertain precise disposition. It is suggested that the process begin with the WHO, the most highly visible office within the EOP.

Recommendation No. 11
It is recommended that a survey be conducted beginning with WHO staff to determine who, in fact, has access to collateral and SCI material. Commensurate levels of clearance and access should be effected and a central record maintained.

Recommendation No. 12
The "White House Office Supplemental Information Sheet for Personnel Action" should be slightly revised as discussed. Inclusion of this information should help speed the process of accessing classified information since Secret/Confidential access can be granted by satisfactory completion of a NACI pending completion of the full field BI.

3. Security Awareness

a. Some procedures are in effect for certain security related issues. For example, page B-6 of the White House Staff Manual outlines how unsecured classified material is to be handled. However, it appears that procedures are neither widely known nor strictly followed. The Security Awareness program should be so designed as to (1) Initially brief incoming personnel, (2) periodically remind employees of their security related responsibilities and (3) brief employees on unique security and CI concerns prior to travel abroad. During the course of this review, several persons commented that "security problems" were most evident in areas populated by "political appointees" as opposed to career civil service/detailed personnel. Most agreed that security awareness training was sorely needed. It was noted, for example, that WHCA offered two

separate briefings on overseas security issues with one person showing up for the first and only a handful for the second. It is also noted that the Security Office, OA, is engaged in a periodic training effort.

Recommendation No. 1
A system-wide program of security training should be initiated. It is suggested that this include briefings to junior and mid-level staff and a comprehensive series of periodic memoranda to senior staff. Emphasis should be placed on the handling and disposal of classified material, classification management and the unique nature of employment within the EOP which may make personnel particularly attractive to Hostile Intelligence Services (HOIS).

Recommendation No. 2
To assist the EOP Security Staff in the conduct of a security awareness program, the Diplomatic Security Service is prepared to present a 45-minute briefing program with Q&As addressing two primary areas: (a) Handling of national security information and (b) Technical security concerns. The latter is designed to demonstrate vulnerabilities of such areas as telephone usage, particularly the ease in interception of conversations on cellular phones.

Recommendation No. 3
The existing 37 minute security awareness instructional tape should be re-done. It is too long, attempts to cover too many unrelated issues and tends to lose the attention of those viewing. It needs to be shortened to a maximum of 15 minutes and considerably tightened in scope and presentation. It should be accompanied by a presentation by each agency security officer addressing agency-specific security issues. It is noted that this effort has been initiated by the OA Security Officer.

Recommendation No. 4
An EOP Security Handbook should be developed and distributed to all current and new personnel. It should include information presented in the tape, contact numbers for security personnel, emergency numbers,

description of procedures and other related information. It is noted that the Security Office, OVP, has developed and issued a detailed and extremely useful document which could provide the basis for an EOP Handbook.

4. Security Organization

a. Virtually every agency within the EOP has its own security coordinator but the entire system is fragmented and lacks cohesion and uniformity. Security procedures vary extensively with minimal cross polination despite periodic meeting of the Security Coordinators group. There is little back-up and when individuals are on travel status procedures slow down and often stop. Uniformity is achieved only on an informal, ad hoc basis. Under a centralized, properly staffed security directorate, policy would be uniform and procedures appropriately enforced.

Recommendation No. 1
To facilitate a comprehensive, EOP-wide security program, it is suggested that the existing fragmented operation be overhauled. For the recommendations made herein to be effective, a change must be made in the way the security program is managed. Therefore, a position should be created to coordinate the wide array of EOP security programs. The primary function would be to establish uniform policy and procedures for all elements within the EOP structure. The incumbent should be a security professional (career or detailed) and the senior security officer within the EOP. The position could be possibly entitled Director of Security, Executive Office of the President, with all existing Security Coordinators reporting to him/her for security programming purposes only. He/She should report to as high a level as possible within the General Counsel, WHO, which will add authority to the function.

Note: To assist EOP Staff in implementing this recommendation, the Diplomatic Security Service is prepared to detail a senior officer to provide guidance and direction as required in establishing such a position.

Attachment: Personnel Interviewed

THE WHITE HOUSE

WASHINGTON

PERSONNEL INTERVIEWED

White House Office
- Mari Anderson, Executive Asst. to WH Per. Sec. Dir.
- Larry W. Croce, Military Office Security Director
- Craig Livingstone, Personnel Security Director
- Beth Nolan, Associate Council to the President
- John D. Podesta, Asst. to the President/Staff Secretary
- Claude A. Taylor, Director of Volunteers
- Paul A. Toback, Special Asst. to Chief of Staff
- Rod Von Lipsey, WH Fellow/Special Asst. to Chief of Staff
- Sharon E. Wagner, Admin. Asst. to the Staff Secretary
- Francis R. Wessel, Admin. Asst. to the Staff Secretary

National Security Council
- James E. Baker, Deputy Legal Advisor
- John W. Ficklin, Deputy Director Records Management
- Christopher L. George, Staff Information Assistant
- David E. Herrington, Adm. Office Systems Director
- Andrew S. Kerr, Staff Information Assistant
- Robert J. Manzanares, Adminstrative Office Director
- Patricia C. Nelson, Security Officer
- John W. Peggins, Systems Manager
- Ralph H. Sigler, Deputy Director WH Situation Room
- David S. Vantassel, Asst. Director Information Disclosure

National Economic Council
- Robert D. Kyle, Special Asst. to the President
- Elaine M. Mitsler, Executive Asst.-International Group

Office of the Vice President
- Todd J. Campbell, Counsel and Dir. of Adm. for the VP
- Joanne M. Hilty, Security Officer for the OVP

Council of Economic Advisors
- Elizabeth A. Kaminski, Admin. Officer and Security Coord.

Office of Administration
- Mary Coutts Beck, Director of Personnel Management
- Christopher D. Cerf, General Council
- Alejandro L. De Leyos, Mailroom Supervisor
- Charles C. Easley, Security Officer
- Mark E. Frownfelder, Security Specialist
- Lawrence R. Jurcich, Telecommunications and Security
- James L. MacDonald, Director Info. Systems and Technology
- Gwendolyn N. Weaver, Dep.Asst. Director for Info. Management

THE WHITE HOUSE

WASHINGTON

Office of Management and Budget
- Roberta L. Foster, Secretary-National Security CCCI
- Darrell A. Johnson, Deputy Asst. Director of Administration
- Marilyn E. Jones, Secretary-Dep. Assoc. Dir. National Sec.
- Anthony B. Wu, Budget Examiner/Acting Branch Chief CCCI

Office of National Drug Control Policy
- Tilman Dean, Support Services Spec./Security Coordinator
- Henry H. Marsden, Director Supply Reduction

Office of Science and Technology Policy
- Barbara A. Ferguson, Administrative Office/Security Coord.
- Deborah J. McGovern, Administrative Assistant
- Joann Ward, Administrative Operations Assistant

President's Foreign Intelligence Advisory Board
- Gwendolyn S. Watson, Administrative Officer/Security Coord.
- Sandra E. Van Namee, Administrative Assistant

United States Trade Representative
- Michael Arbogast, Systems Analyst
- Lorraine Green, Human Resources Manager
- Catherine A. Hofgren, Sup. Servs. Supervisor/Security Coord.
- David Spetrino, Special Asst. to the USTR
- Joan C. Steyaert, Director Computer Operations

White House Communications Agency
- Francis Bartol, Communications Center
- Paul Connelly, Security Officer
- Robert Gutjahr, Deputy Security Officer
- Lawrence Ledbetter, Communications Center

United States Secret Service
- Arnie Cole, WH Sec. Branch-Investigations/Access Controls
- Lt. Ron Elie, WH Uniformed Division
- Tom Farrell, WH Security Branch Chief
- Capt. Flanagen, WH Uniformed Division
- Capt. J.J. Hampton, WH Uniformed Division
- Officer Richard Tozier, WH Uniformed Division
- Don Flynn, WH Security Branch
- John J. Robey, Technical Services Branch Chief

General Services Administration
- Lawrence Downes, Shredder Room NEOB

SENSITIVE BUT UNCLASSIFIED

TO: Mr. Christopher D. Cerf
White House Counsel's Office
Executive Office of the President

May 27, 1994

FROM: Christopher M.B. Disney CD
John R. Hancock JRH
Bureau of Diplomatic Security
US Department of State

SUBJ: Review of EOP Security Issues

The Bureau of Diplomatic Security of the Department of State was informally requested to assist the Executive Office of the President in conducting a review of procedures involving the handling and storage of national security information. The review was conducted during the period May 16-27, 1994, by the reporting officers who were detailed to the EOP for the duration of the review.

The review was necessarily limited in scope due to time restrictions but, in all, 62 interviews were conducted as shown on the attached listing of personnel. In addition to interviewing EOP personnel, including detailees, an after hours review of USSS-UD security check procedures was conducted. Documentation reviewed included items such as the White House Staff Manual, OPM instructions and a variety of EOP security-related memoranda.

It is the opinion of reporting officers that, in general, procedures governing the handling of national security information ranged from highly effective to those requiring improvement. Certain EOP elements such as the NSC, WHMO, ONDCP, PFIAB and others which handle large quantities of classified information appeared to have viable, pro-active and aggressive security programs. Procedures reviewed within these elements adhere to USG regulations and commonly accepted practice. Officers charged with security responsibilities are well versed in procedure and provided

evidence of well-structured, detailed and thorough programs. All personnel interviewed displayed extremely positive attitudes towards the conduct of the review and voiced the expected commitment towards the protection of classified and sensitive information.

Areas requiring improvement and modification of procedure are addressed in the attached outline. We found that only certain security practices and procedures generally involving offices not handling large quantities of classified information needed attention. Corrective action, in most cases, could be achieved by an aggressive security awareness training program and revision of some procedures. In addition, the recommended consolidation of security functions would provide a comprehensive, uniform and centrally-managed approach with clear lines of authority and responsibility.

The issues addressed and recommendations which resulted are divided into four general areas: (1) Procedural Security, (2) Personnel Security, (3) Security Awareness and (4) Security Organization.

1. Procedural Security

a. Protection of national security information was the major purpose of this review. Most EOP elements indicated their handling of classified information was minimal. Examination disclosed procedures which ranged from highly effective to those requiring improvement.

A common set of procedures addressing the accessing, handling and disposal of classified information does not exist. Procedures have been issued by the EOP Security Officer within the Office of Administration for certain EOP offices but they are dated (June 1988) and have not been established for or applied to all elements of the EOP. Several organizations within the EOP appear to lack formal procedures for governing the access and handling of national security information.

Recommendation No. 1
Uniform procedures based upon existing USG regulations should be drafted and promulgated to all entities which comprise the Executive Office of the President.

b. Classified information enters EOP elements either electronically (classified communications circuits or secure fax) or hand-carried by courier. In each of the entities of the EOP structure, material is ordinarily distributed from a central distribution point or is received through a terminal in a SCIF. Highly sensitive material, for example the NID, appears for the most part to receive the requisite handling and protection with the exception that in some cases the NID is not returned in a timely manner causing extensive administrative problems in conducting the necessary tracking procedure. In one case, the NID had not been returned for almost six months. In another case, the NID was routinely included in a comprehensive daily briefing book and given to a secretary for further distribution. This person is not, as of the date of this report, cleared for access to SCI.

Recommendation No. 2
All recipients of the NID and other numerically controlled documents should be reminded by memorandum from as high a level as appropriate of their obligation to restrict access to this material and return these documents to the issuing office within the prescribed time period. In addition, strict adherence must be maintained to the limitations placed upon distribution of the NID by the CIA. Access by personnel not on the distribution list must be approved by the originating office within CIA.

c. Within the EOP, outside the NSC, WHMO, PFIAB, ONDCP and a few other exceptions, there appears to be remarkably little national security information processed and stored. There is, however, a significant amount of information which is extremely sensitive in nature -- the President's Daily Schedule is one example. Anecdotally, during reporting officers' assignment to the OEOB, part of the time was spent in Room 502. Each morning a copy of the President's Schedule for that day and, on one occasion, a 3-month advance schedule was found in an envelope in front of Room 502 marked for "Jeff Watson" who presumably formerly occupied the office. The Schedule was unclassified and uncontrolled in an unsealed envelope.

Recommendation No. 3
Procedures for limiting distribution and enhancing protection of sensitive information, especially the President's Daily Schedule, should be reviewed and improvements made as appropriate. This process should also extend to information transmitted by unclas fax between the White House Complex and Presidential trip site locations.

d. Personnel interviewed were aware and acknowledged that the EOP/OA computer system in use (OASIS), was restricted to unclassified information. However, if secure systems did not exist in their office space, not all personnel were aware how classified information could be processed. It is noted that the IST Division of OA has recently completed

a draft directive on InfoSec concerns. It appears thorough, detailed and broad in scope and should be promulgated as soon as possible.

Recommendation No. 4
Procedures should be issued reinforcing the requirement not to process classified information on non-secure systems. Personnel should also be made aware of available automated systems which can be utilized for processing classified information and the highest level of information permitted.

e. Procedures for disposition of classifed material in many office areas seemed unclear. Cursory reviews of many office spaces detected unusually few security containers.

Recommendation No. 5
A thorough survey should be conducted by each agency/office security officer to determine the exact requirement for security containers with an emphasis on reducing any classified holdings to the greatest extent possible but insuring that the remainder receive appropriate storage in approved containers. In addition, combinations on all security containers should be changed upon the departure of the office incumbent and/or at least once a year. Records should be maintained. It may be beneficial to have one or more common security containers located in the West Wing first and second floor areas where classified can be stored as required. It is also noted that SCIFs are not established on these two floors. All SCI material must, therefore, be secured in the Sit Room on the ground floor.

f. Few offices are equipped with shredders; most rely on burn bags. Discussions with a variety of employees revealed an inconsistent approach to the burn bag process. Some were collected by USSS-UD and others were delivered to a central shredding facility. Some employees seemed unsure of the process and used burn bags for disposal of unclassified material. Anecdotally, reporting officers discovered an unsecured burn bag in an unoccupied office in the OEOB at OOB on a Monday

morning. It was not checked for classified material. It had been unprotected for an unknown period over a week-end.

Recommendation No. 6
Clear, consistent procedures should be established for the collection/ disposal of classified waste material. Ensure "open storage" is not permitted in unauthorized spaces. Each office which processes/handles classified information should utilize a standardized COB check list. After hours checks by USSS-UD should include checking for unsecured burn bags, classified information left unprotected and open containers.

Recommendation No. 7
Instructions issued on May 16, 1994 by Ms. Patsy Thomasson should be enforced. The shredder operator at the NEOB complained that burn bags continue to be piled in front of his door at OOB each morning. Each would have been unprotected on an unsecure loading dock area for varying periods and therefore subject to compromise.

g. Hard copy material is hand-carried throughout the EOP complex which includes the NEOB, the OEOB, the Winder Building, ONDCP and the White House. Procedures lack uniformity and vary in the degree of protection afforded. The EOP Mail Room process (Red Tag) appears effective but personnel from many offices also individually hand deliver material.

Recommendation No. 8
Instructions should be issued clarifying courier procedures and lockable courier pouches should be issued to central offices within each building for the transport of SCI material. Personnel transporting classified/ sensitive information outside the OEOB/WH complex should be reminded of requirements and procedures.

Recommendation No. 9
Storage/access procedures for SCI and other codeword material should be thoroughly examined especially in West Wing offices. A walk-through by reporting officers at 2300 hours on 5/25 disclosed the fact that (a) few,

if any, safes are available in West Wing working spaces, and (b) at COB, within certain West Wing first floor offices, material was simply left on the desk - a TS document was discovered unprotected on one desk. It is noted, however, that a UD officer is present in front of the Oval Office 24 hours a day making the possibility of compromise remote. Due to the quantity of documents seen unprotected in various offices, the presence of other collateral or code word material cannot be discounted.

Recommendation No. 10
New COB procedures should be established for certain first floor West Wing offices. After departure of the principal, staff members should be required to collect all classified/sensitive material and secure it. Safes should be procured for this purpose. While access to the West Wing is controlled by UD personnel and chars are escorted (ratio unknown), material left exposed could be subjected to scrutiny by char force or other uncleared personnel perhaps being escorted on tours.

Recommendation No. 11
Certain offices have evening secretarial shifts. If the secretary leaves prior to collection of the burn bag by the UD officer, she simply leaves the unsecured bag in full view. This procedure is also employed by day shift personnel. Burn bags should receive more positive control. One option would be for staff members to hand carry the closed burn bag to a central holding room for later collection by UD. This will insure positive control from the time a document enters the office to its destruction.

Recommendation No. 12
Within the EOP, burn bag destruction procedures fall into two general categories: (1) NSC (both Sit Room and OEOB) material is held in a secure area for weekly collection and destruction by CIA courier, and (2) Collection by UD personnel and office staff and carriage to one of two destruction facilities in the OEOB (Basement Area) or NEOB (Loading Dock). In the latter category, material is taken out of the burn bag and placed on the conveyor belt which carries it to the shredder. At that point the material is in full view of the operator. SCI material may be present and operators have not been authorized SCI access. Either operators should be

SCI accessed or instructions should be promulgated to staff to segregate SCI from collateral waste.

2. Personnel Security

a. Within the White House Personnel Security Office (WHPS), a 17-step process has been established which results in the issuance of a building pass. In addition, under the signature of the Chief of Staff, an instruction was issued on March 14, 1994 concerning completion of security related paperwork for new employees. Procedures seem clear, are endorsed by senior management and provide for punitive measures for non-compliance. The areas which may warrant additional attention, however, are the adjudication process and the timeliness of the entire procedure. The FBI conducts a SSBI and returns the ROI to the WHPS where it is reviewed for issues of suitability and potential embarrassment to the Administration. The report is then forwarded to the USSS for review from a protective intelligence perspective and a permanent pass issued as appropriate.

The pass that is issued appears to be adjudicated primarily on the basis of suitability and potential threat to the President. While not dissimilar, adjudicative criteria for access to national security information which would include potential CI concerns does not appear to be specifically addressed in this process. Issuance of the pass, however, is in fact viewed as the potential for authority to access classified information up to and including Top Secret. There is some confusion as to exactly what issuance of a permanent pass means.

Recommendation No. 1
The system employed by the various elements of the EOP to issue building passes and to grant clearances lacks uniformity. While unique requirements exist, for example, within the WHO and WHMO, procedures should be as common as possible. A Task Force composed of EOP Security and Personnel Officers should address this issue and arrive at consensus.

Redundant areas should be identified and avoided. N.B. During the course of the review, several comments were made regarding the excessive length of the clearance process which caused administrative problems. It is noted, however, that a great deal of attention has been given to this issue and as of May 11th, 76% of the staff had been issued passes. The balance were either in the adjudication process, pending a BI or awaiting paperwork (2%).

Recommendation No. 2
If, in the adjudication process, a conscious application of criteria governing access to national security information is not applied, then this should occur forthwith. Personnel involved in the adjudication process should refamiliarize themselves with these instructions which are included in Chapters 731, 732, 735 and 736 of the Federal Personnel Manual as amended by the FPM Sunset Document.

Note: The Diplomatic Security Service is prepared to detail a senior Personnel Security Adjudicator to work within the WHPS for a short period to assist in the establishment of this process and provide informal OJT of personnel as necessary.

Recommendation No. 3
To assist in the timely retrieval of information concerning the level of clearance granted/held by each employee who is a member of any element of the EOP or who holds any type of pass allowing unescorted access to any EOP facility, a data base should be created. Information should be available in this system to any of the security officers within the EOP structure. This will also aid considerably in the passing of clearances in a timely fashion to other USG agencies.

Recommendation No. 4
Signing of the SF 312 and the resulting acknowledgement of one's responsibilities in the protection of classified information is inconsistent. Throughout the EOP, common procedures should be established in the clearance issuance and briefing process to insure the SF 312 is signed by each person granted access to classified material.

Recommendation No. 5
The building pass system seemed unnecessarily complicated with a somewhat bewildering array of variously colored and lettered passes. The brevity of this survey did not permit a detailed analysis of the system but it is recommended that this issue be another agenda item for the EOP Security Coordinator group to address.

Recommendation No. 6
Employment of Volunteers and Interns in areas in which classified material is handled should be severely limited. If unavoidable, those so employed should be cleared up to the Secret level with access limited to that level. This can be accomplished through conduct of a NACI.

Recommendation No. 7
The wording of the memorandum from WHPS regarding the completion of a favorable BI and the authorization for a permanent building pass and security clearance should be revised. It is imprecise and is not understood by at least one EOP unit security officer.

Recommendation No. 8
WHPS personnel are under pressure to insure that personnel are cleared in as short a time frame as possible. Given the functions expected of this office, it appears extremely understaffed and in unusually cramped physical space. Efforts to alleviate both problems should be undertaken as soon as possible.

Recommendation No 9
The WHPS staff is required to adjudicate a wide variety and a vast number of background investigations. The process ultimately allows access to national security information. All EOP personnel, especially those in the WHPS, who are charged with adjudicative responsibility should receive formalized training. It is recommended that this occur to insure proper criteria is applied and to maintain the credibility of the process.

Recommendation No. 10
It is recommended that a program be initiated as soon as possible to subject each file on the pending clearance/building pass list to a thorough review to ascertain precise disposition. It is suggested that the process begin with the WHO, the most highly visible office within the EOP.

Recommendation No. 11
It is recommended that a survey be conducted beginning with WHO staff to determine who, in fact, has access to collateral and SCI material. Commensurate levels of clearance and access should be effected and a central record maintained.

Recommendation No. 12
The "White House Office Supplemental Information Sheet for Personnel Action" should be slightly revised as discussed. Inclusion of this information should help speed the process of accessing classified information since Secret/Confidential access can be granted by satisfactory completion of a NACI pending completion of the full field BI.

3. <u>Security Awareness</u>

a. Some procedures are in effect for certain security related issues. For example, page B-6 of the White House Staff Manual outlines how unsecured classified material is to be handled. However, it appears that procedures are neither widely known nor strictly followed. The Security Awareness program should be so designed as to (1) Initially brief incoming personnel, (2) periodically remind employees of their security related responsibilities and (3) brief employees on unique security and CI concerns prior to travel abroad. During the course of this review, several persons commented that "security problems" were most evident in areas populated by "political appointees" as opposed to career civil service/detailed personnel. Most agreed that security awareness training was sorely needed. It was noted, for example, that WHCA offered two

separate briefings on overseas security issues with one person showing up for the first and only a handful for the second. It is also noted that the Security Office, OA, is engaged in a periodic training effort.

Recommendation No. 1
A system-wide program of security training should be initiated. It is suggested that this include briefings to junior and mid-level staff and a comprehensive series of periodic memoranda to senior staff. Emphasis should be placed on the handling and disposal of classified material, classification management and the unique nature of employment within the EOP which may make personnel particularly attractive to Hostile Intelligence Services (HOIS).

Recommendation No. 2
To assist the EOP Security Staff in the conduct of a security awareness program, the Diplomatic Security Service is prepared to present a 45-minute briefing program with Q&As addressing two primary areas: (a) Handling of national security information and (b) Technical security concerns. The latter is designed to demonstrate vulnerabilities of such areas as telephone usage, particularly the ease in interception of conversations on cellular phones.

Recommendation No. 3
The existing 37 minute security awareness instructional tape should be re-done. It is too long, attempts to cover too many unrelated issues and tends to lose the attention of those viewing. It needs to be shortened to a maximum of 15 minutes and considerably tightened in scope and presentation. It should be accompanied by a presentation by each agency security officer addressing agency-specific security issues. It is noted that this effort has been initiated by the OA Security Officer.

Recommendation No. 4
An EOP Security Handbook should be developed and distributed to all current and new personnel. It should include information presented in the tape, contact numbers for security personnel, emergency numbers,

description of procedures and other related information. It is noted that the Security Office, OVP, has developed and issued a detailed and extremely useful document which could provide the basis for an EOP Handbook.

4. Security Organization

a. Virtually every agency within the EOP has its own security coordinator but the entire system is fragmented and lacks cohesion and uniformity. Security procedures vary extensively with minimal cross polination despite periodic meeting of the Security Coordinators group. There is little back-up and when individuals are on travel status procedures slow down and often stop. Uniformity is achieved only on an informal, ad hoc basis. Under a centralized, properly staffed security directorate, policy would be uniform and procedures appropriately enforced.

Recommendation No. 1
To facilitate a comprehensive, EOP-wide security program, it is suggested that the existing fragmented operation be overhauled. For the recommendations made herein to be effective, a change must be made in the way the security program is managed. Therefore, a position should be created to coordinate the wide array of EOP security programs. The primary function would be to establish uniform policy and procedures for all elements within the EOP structure. The incumbent should be a security professional (career or detailed) and the senior security officer within the EOP. The position could be possibly entitled Director of Security, Executive Office of the President, with all existing Security Coordinators reporting to him/her for security programming purposes only. He/She should report to as high a level as possible within the General Counsel, WHO, which will add authority to the function.

Note: To assist EOP Staff in implementing this recommendation, the Diplomatic Security Service is prepared to detail a senior officer to provide guidance and direction as required in establishing such a position.

Attachment: Personnel Interviewed

THE WHITE HOUSE

WASHINGTON

PERSONNEL INTERVIEWED

White House Office
- Mari Anderson, Executive Asst. to WH Per. Sec. Dir.
- Larry W. Croce, Military Office Security Director
- Craig Livingstone, Personnel Security Director
- Beth Nolan, Associate Council to the President
- John D. Podesta, Asst. to the President/Staff Secretary
- Claude A. Taylor, Director of Volunteers
- Paul A. Toback, Special Asst. to Chief of Staff
- Rod Von Lipsey, WH Fellow/Special Asst. to Chief of Staff
- Sharon E. Wagner, Admin. Asst. to the Staff Secretary
- Francis R. Wessel, Admin. Asst. to the Staff Secretary

National Security Council
- James E. Baker, Deputy Legal Advisor
- John W. Ficklin, Deputy Director Records Management
- Christopher L. George, Staff Information Assistant
- David E. Herrington, Adm. Office Systems Director
- Andrew S. Kerr, Staff Information Assistant
- Robert J. Manzanares, Adminstrative Office Director
- Patricia C. Nelson, Security Officer
- John W. Peggins, Systems Manager
- Ralph H. Sigler, Deputy Director WH Situation Room
- David S. Vantassel, Asst. Director Information Disclosure

National Economic Council
- Robert D. Kyle, Special Asst. to the President
- Elaine M. Mitsler, Executive Asst.-International Group

Office of the Vice President
- Todd J. Campbell, Counsel and Dir. of Adm. for the VP
- Joanne M. Hilty, Security Officer for the OVP

Council of Economic Advisors
- Elizabeth A. Kaminski, Admin. Officer and Security Coord.

Office of Administration
- Mary Coutts Beck, Director of Personnel Management
- Christopher D. Cerf, General Council
- Alejandro L. De Leyos, Mailroom Supervisor
- Charles C. Easley, Security Officer
- Mark E. Frownfelder, Security Specialist
- Lawrence R. Jurcich, Telecommunications and Security
- James L. MacDonald, Director Info. Systems and Technology
- Gwendolyn N. Weaver, Dep.Asst. Director for Info. Management

THE WHITE HOUSE

WASHINGTON

Office of Management and Budget
- Roberta L. Foster, Secretary-National Security CCCI
- Darrell A. Johnson, Deputy Asst. Director of Administration
- Marilyn E. Jones, Secretary-Dep. Assoc. Dir. National Sec.
- Anthony B. Wu, Budget Examiner/Acting Branch Chief CCCI

Office of National Drug Control Policy
- Tilman Dean, Support Services Spec./Security Coordinator
- Henry H. Marsden, Director Supply Reduction

Office of Science and Technology Policy
- Barbara A. Ferguson, Administrative Office/Security Coord.
- Deborah J. McGovern, Administrative Assistant
- Joann Ward, Administrative Operations Assistant

President's Foreign Intelligence Advisory Board
- Gwendolyn S. Watson, Administrative Officer/Security Coord.
- Sandra E. Van Namee, Administrative Assistant

United States Trade Representative
- Michael Arbogast, Systems Analyst
- Lorraine Green, Human Resources Manager
- Catherine A. Hofgren, Sup. Servs. Supervisor/Security Coord.
- David Spetrino, Special Asst. to the USTR
- Joan C. Steyaert, Director Computer Operations

White House Communications Agency
- Francis Bartol, Communications Center
- Paul Connelly, Security Officer
- Robert Gutjahr, Deputy Security Officer
- Lawrence Ledbetter, Communications Center

United States Secret Service
- Arnie Cole, WH Sec. Branch-Investigations/Access Controls
- Lt. Ron Elie, WH Uniformed Division
- Tom Farrell, WH Security Branch Chief
- Capt. Flanagen, WH Uniformed Division
- Capt. J.J. Hampton, WH Uniformed Division
- Officer Richard Tozier, WH Uniformed Division
- Don Flynn, WH Security Branch
- John J. Robey, Technical Services Branch Chief

General Services Administration
- Lawrence Downes, Shredder Room NEOB