

FOIA MARKER

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

Folder Title:

Personnel Security [9]

Staff Office-Individual:

Legal Advisor-Derosa, Mary

Original OA/ID Number:

4058

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

Withdrawal/Redaction Sheet

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001a. memo	For Security Policy Board members and observers. [partial] [CIA Act] (1 page)	09/12/1995	P3/b(3)
001b. list	Addressees. [partial] [CIA Act] (1 page)	09/12/1995	P3/b(3)
002. fax	Cover Sheet. List of Addressees. [partial] [CIA Act] [10 U.S.C. §424] [National Security Act] (1 page)	08/18/1995	P3/b(3)

COLLECTION:

Clinton Presidential Records
National Security Council
Legal Advisor (Mary DeRosa)
OA/Box Number: 4058

FOLDER TITLE:

Personnel Security [9]

2006-1066-F

vz877

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]

11112

INTERNAL PROCEDURES FOR
ACCESS TO CLASSIFIED INFORMATION

In accordance with EO _____, dated _____, the following procedures for granting access to classified information will be followed within the White House Complex:

Section 1.1: Definitions: See EO _____.

Section 1.2: Access to Classified Information.

(a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with EO _____, and to possess a valid need-to-know to perform one's official White House Duties.

*Was not
fit -
qualify ->*
(b) The Security Officer, Executive Office of the President, in coordination with each agency, shall establish and maintain an effective program to ensure that access to classified information is consistent with the interest of national security.

*What about
exceptions ->*
(c) Access to classified information shall be limited to employees who:

(1) are citizens of the United States;

(2) have been determined to be eligible for access under section 3.1(b), by the Security Officer, Executive Office of the President upon a favorable adjudication of an appropriate investigation of the employee's background;

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

(4) have signed an approved non-disclosure agreement.

(d) All employees shall be subject to an investigation by the FBI, or other authorized investigative agencies, prior to being granted access to classified information. Reinvestigations will be completed at five year intervals, or at any time an issue regarding an individuals suitability for continuing access to classified information is raised.

as appropriate
(e) All individuals, upon selection for employment/volunteer/intern/detailee/fellow/consultant to The Executive Office of the President shall submit to the EOP Security Office, or the White House Personnel Security Office, a:

- (1) completed Standard Form 86,
- (2) IRS Tax Wavier form,
- ? → (3) file a financial disclosure report, including information with respect to the spouse and dependent children of the employee,
- ? (4) for those employees undergoing a five year re-investigation, file an annual financial disclosure report,
- (5) file relevant information concerning foreign travel as determined by the Security Policy Board, and
- (6) provide written consent to the employing agency permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of three years thereafter,

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

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

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

- ? (2) Information may be requested pursuant to employment if:

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

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

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

- (3) Nothing in this section shall be construed to affect the

authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act, the Fair Credit Reporting Act or any other applicable law.

(4) Upon receipt of the completed security forms the EOP Security Office or White House Personnel Security Office, will:

- removed
supplies →*
- (a) initiate the appropriate background investigation, *verify?*
 - (b) initiate the tax check report with the IRS,
 - (c) coordinate, with the appropriate counsel's office, for a review of the financial disclosure statements.

Sect 1.3 Financial Disclosure:

*Part of
in - brief*

(a) Each agency within the EOP that originates, handles, or transmits, or possesses classified information shall identify in writing to the EOP Security Office, each employee, by position or category where possible, who requires access to information that, at the discretion of the agency head, would reveal:

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

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

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

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

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

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

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

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

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

Sect 1.4 Use of Automated Financial Record Data Bases>

? W/WHITE HOUSE

Sect 1.5 Employee Education and Assistance.

The EOP Security Officer will establish and maintain an ongoing security education program consisting of the following:

(a) a monthly security briefing for all new employees.

Required? (b) annual security refresher briefing for all employees who have been granted access to classified information.

(c) provide specialized security training or briefings as required.

(d) provide a security indoctrination that covers the handling, transmittal and storage of classified information to each employee upon granting of a security clearance.

(e) provide guidance and assistance to individuals concerning issues that may affect their eligibility for access or continuing access to classified information.

Under Individuals who have questions or concerns about financial matters, mental health, or substance abuse will be referred to the EOP Employee Assistance Program (EAP), and/or to a consumer counselling service.

Part 2

Access Eligibility Policy and Procedures

Sect. 2.1 Eligibility Determinations.

(a) Determinations of eligibility for access to classified information shall be based on the adjudication of a favorable background investigation, and a clearly defined need-to-know to perform one's official assigned duties within the White House Complex. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment within the EOP.

(b) The number of employees granted access to classified information will be kept to an absolute minimum consistent with the operational requirements of each office or agency within the EOP.

(1) Security clearance request will be submitted to the appropriate security office, using the format in enclosure 1.

(2) Eligibility for access to classified information will not be requested or granted solely to permit entry to, or ease of movement within the White House Complex. Special consideration may be given when circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties. Request for special consideration will be handled on a case by case basis after coordination between the EOP Security Office, White House Counsel, and the office of employment.

(3) Request for access to classified information may be granted where there is a temporary need for access, such as a one-time participation in a classified project, and provided the investigative standards established under EO 12958 have been satisfied. Such request will be forwarded to the EOP Security Officer, with a fixed date or event for expiration. If approved, access to classified information will be limited to information related to the particular project or assignment.

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

Sect 2.2 Level of Access Approval.

(a) The level at which access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Request for a security clearance will be submitted to the appropriate security office using the format shown in enclosure 1. This request must be signed by a senior manager. The number and level of clearances will be kept to an absolute minimum consistent with operational requirements. Upon approval the security clearance will be granted using the format in Enclosure _____. A copy of the clearance approval will be given the individual, placed in the individual's

official personnel file and security file, and to the office or agency of employment.

NSC?
rule

(b) Request for access to special access programs (SAP) (Intelligence or Department of Energy activities) will be submitted in writing, with a brief justification, to the appropriate security office. Once a clearly defined need-to-know has been established, and a determination made that the individual meets the security requirements to the SAP, the request will be forwarded to the agency for consideration. The number of employees granted access to SAP will be kept to an absolute minimum consistent with operational requirements.

Sect 2.3 Temporary Access to Higher Levels.

(a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation my be granted temporary access to a higher level upon written request to the appropriate security office, where such access:

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

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

Sect 2.4 Reciprocal Acceptance of Access Eligibility Determinations.

NO
discuss

(a) Will the White House continue to have the FBI conduct background investigations even when a current background investigation has been completed by another investigative agency.

(b) if not, then the current background investigation can be used to grant security clearances.

Sect 2.5 Specific Access Requirements.

(a) Employees who have been determined to be eligible for access to classified information shall be given access only when there is a clearly defined need-to-know in order to conduct official duties.

(b) It is the responsibility of any employee who has been

authorized to maintain classified information to verify that prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

The EOP Security Office can verify security clearances for all personnel within the White House Complex.

Sect 2.6 Access by Non-United States Citizens.

Answers { (a) All employees of the EOP are required to be United States Citizens, therefore there will be no requirement to grant access to classified information to someone who is not a citizen. -?

(b) Any exceptions to this requirement must be approved by the Deputy Assistant to the President for Management and Administration.

Part 3

Access Eligibility Standards

Sect. 3.1 Standards.

The EOP will follow the adjudication guidelines to be established by the Security Policy Board.

*specific
or not*

Sect 3.2 Basis for Eligibility Approval.

(a) Eligibility determinations for access to classified information shall be based ^{upon} the following:

review { (1) favorable adjudication of a completed background investigation.

(2) favorable review of appropriate financial disclosures records by the agency's General Counsel.

(3) if required, favorable checks with other financial and travel institutions.

(b) The EOP Security Officer will conduct personal interviews, if needed, to clarify information or to help resolve any issues developed by the investigation. Additional investigations will be initiated if required.

Sect 3.3 Special Circumstances.

(a) Temporary eligibility can be granted in special cases when it is determined by an agency head that the mission of the agency would be adversely affected if an individual is not granted immediate access to classified information.

EOP ethics had a in case of WFO

(1) Request for temporary eligibility for access must include a justification, and be submitted in writing to the EOP Security Officer.

(b) Temporary eligibility for access will only be granted after:

(1) completion of a pre-employment interview.

(2) completion of a favorable FBI name check.

(3) review of the completed security forms; and

(4) initiation of the appropriate background investigation.

(5) attendance of the White House Security Briefing for new employees.

(c) Temporary eligibility will be granted in writing (Enclosure _____). A copy of this determination will be placed in the individual's official personnel file, security file, and copy provided to the agency concerned.

(d) Where access has been terminated, and a new need arises, access eligibility can be reapproved without further investigations provide the investigation was completed within the last five years, and they have remained employed by the EOP. The employee will be required to review the latest Standard Form (SF) 86, and make changes as appropriate.

(e) Access eligibility can be approved for former government employees provided they have not been outside government service for more then two years, and the background investigation was completed within the last five years. The individual must provide a copy of the latest SF-86, and make changes as appropriate.

Sect. 3.4. Reinvestigation Requirements.

(a) All employees within the White House Complex will be the subject of a periodic reinvestigation every five years. A reinvestigation may also be requested at any time there is reason to believe the individual may no longer meet the standards for access to classified information, or to the White House Complex.

(b) The EOP will follow the reinvestigation standards to be established by the Security Policy Board.

(c) Information that raises doubts as to whether an employee's continued eligibility for access to classified information should be forwarded immediately to the EOP

By whom?
Series
FBI for
PUC
CRS

Security Office.

Part 5 Review of Access Determinations.

Sect 5.1. Determinations of Need for Access.

Sect 5.2. Determinations of Eligibility for Access.

Link to EOP process not good

(a) The EOP Security Officer, in coordination with White House Counsel, and the appropriate agency General Counsel will make the determination if an employee is not eligible for access to classified information:

(1) The EOP Security Officer will provide a comprehensive and detailed written explanation of the basis for that conclusion as the national security interests of the United States and other applicable laws permit.

? → (2) The individual has the right to be represented by counsel, at their own expense.

(3) The individual will have 10 working days to reply in writing, and to request a review of the determination.

(4) Provide the employee with written results of the review, and identify the deciding authority.

Link

(5) Provide the individual with the opportunity to appeal in writing to a high level panel. This panel will be appointed by the agency head, or in case of a White House employee (~~WH GC~~). The panel shall be comprised of at least three members, two of whom must be selected from outside the security field. Decisions of the panel shall be final.

Note sent exceptor?

(6) The individual will be provided with an opportunity to appear personally before the panel.

not required

Part 6 Implementation

Sect. 6.1 Agency Implementing Responsibilities.

(a) The EOP Security Officer will be responsible for administering the personnel security program within the White House Complex which shall include:

(1) Active oversight and continuing security awareness program.

(2) Coordination with the US Secret Service in the conduct of after hours security inspections of offices

what about Detolless Sinfy

in the West and East Wings, Old Executive Office and New Executive Office Buildings and Federal Protective Service for office space in the Winder Building.

→ (3) Maintain liaison with the Security Policy Board.

(4) Maintain liaison with the Information Security Oversight Office.

(5) Conduct periodic evaluations of each agency's procedures for handling and processing classified information.

Sect 6.2 Employee Responsibilities.

Employees who have been granted access to classified information will receive a security indoctrination at the same time they are granted access. At the same time they will be provided with a hand out (Enclosure ____) explaining some of their responsibilities.

Sect 6.3 Sanctions. **PER E^o**

Define EOP sent office

S- A- M- P- L- E

MEMORANDUM FOR THE EOP SECURITY OFFICER

FROM: _____

SUBJECT: Access to Classified Information

I have determined that _____ an employee
of _____ (Name)
_____ will require access
(Office/Agency)
to classified information at the _____
(SECRET or TOP SECRET)

level.

Upon favorably adjudication of the individual's background investigation, I understand that the EOP Security Officer will:

1. Have the individual complete an SF-312 (Non-Disclosure Agreement).
2. Provide appropriate security indoctrination to insure the individual is knowledgeable of procedures for handling and storage of classified documents.
3. Provide my office with the date and level of the security clearance granted.

(Signature)

(Title/Position)

(Date)

(date)

SECURITY DETERMINATION

NAME: DOE, John J.

DPOB: 12-25-66, Anytown, USA

POSITION: Job Title

AGENCY: Office of Agency

INVESTIGATION

TYPE: Background Investigation

COMPLETED BY: FBI

DATE COMPLETED: (date)

CLEARANCE GRANTED: (date)

THE ABOVE NAMED INDIVIDUAL HAS BEEN GRANTED SECURITY APPROVAL BY THE EXECUTIVE OFFICE OF THE PRESIDENT AND IS AUTHORIZED TO HAVE ACCESS TO CLASSIFIED INFORMATION THROUGH (SECRET) (TOP SECRET). THIS IS GRANTED UNDER THE STANDARDS OF EXECUTIVE ORDER 10450.

CHARLES C. EASLEY
EOP SECURITY OFFICER

CERTIFICATION

I CERTIFY THAT HAVE BEEN BRIEFED ON THE PROCEDURES FOR HANDLING, STORAGE AND TRANSMISSION OF CLASSIFIED INFORMATION IN ACCORDANCE WITH EO 12958, AND THAT I HAVE READ AND COMPLETED A NON-DISCLOSURE AGREEMENT (SF-312).

(DATE)

(SIGNATURE)

DISTRIBUTION:

- 1 - OFFICIAL PERSONNEL FILE
- 1 - SECURITY FILE
- 1 - OFFICE OF ASSIGNMENT
- 1 - INDIVIDUAL

(date)

SECURITY DETERMINATION

NAME: DOE, John J.
DPOB: 12-25-66, Anytown, USA
POSITION: Job Title
AGENCY: Office of Agency

INVESTIGATION

TYPE: Background Investigation COMPLETED BY: FBI
DATE INITIATED: (date) CLEARANCE GRANTED: (date)

THE ABOVE NAMED INDIVIDUAL HAS BEEN GRANTED TEMPORARY SECURITY APPROVAL BY THE EXECUTIVE OFFICE OF THE PRESIDENT AND IS AUTHORIZED TO HAVE ACCESS TO CLASSIFIED INFORMATION THROUGH (SECRET) (TOP SECRET). THIS IS GRANTED UNDER THE STANDARDS OF EXECUTIVE ORDER 10450.

CHARLES C. EASLEY
EOP SECURITY OFFICER

CERTIFICATION

I CERTIFY THAT HAVE BEEN BRIEFED ON THE PROCEDURES FOR HANDLING, STORAGE AND TRANSMISSION OF CLASSIFIED INFORMATION IN ACCORDANCE WITH EO 12958, AND THAT I HAVE READ AND COMPLETED A NON-DISCLOSURE AGREEMENT (SF-312). I ALSO UNDERSTAND THAT FURTHER ACCESS IS EXPRESSLY CONDITIONED ON THE FAVORABLE COMPLETION OF THE BACKGROUND INVESTIGATION AND ISSUANCE OF AN ACCESS ELIGIBILITY APPROVAL, AND THAT ACCESS WILL BE IMMEDIATELY TERMINATED, ALONG WITH ANY ASSIGNMENT REQUIRING AN ACCESS ELIGIBILITY APPROVAL, IF SUCH ELIGIBILITY IS NOT GRANTED.

(DATE)

(SIGNATURE)

DISTRIBUTION:

- 1 - OFFICIAL PERSONNEL FILE
- 1 - SECURITY FILE
- 1 - OFFICE OF ASSIGNMENT
- 1 - INDIVIDUAL

(DATE)

I understand that by granting me access to classified information the Executive Office of the President (EOP) has placed a special trust in me. By accepting this responsibility I agree to the following:

- a. I will protect all classified information in my custody from unauthorized disclosure.
- b. I will ensure that all classified information in my custody is locked in an approved security container or approved vaulted area when unattended.
- c. I will report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information
- d. I will report all violations of security regulations and/or procedures to the appropriate security official.
- e. I realize that classified information is the sole property of the United States Government, and cannot be used for personal gain.
- f. I understand that classified information must be stored in approved containers and cannot be taken to my home.
- g. I will comply with all security requirements set forth by the Executive Office of the President, and all rules and regulations governing the protection of classified information.

Date)

(Signature)

Baker, James E.

From: Appel, Edward J.
To: Baker, James E.
Cc: /R, Record at A1; Beers, Rand R
Subject: SF-86 Background Investigation Scope [UNCLASSIFIED]
Date: Thursday, August 31, 1995 9:54AM

Jamie,

As I think we discussed briefly before, OMB is concerned that the 7-year scope of the new SF-86 background forms conflicts with the standing EO on the subject (an old one), which calls for a ten-year scope. As the SPB provides standards and parameters for backgrounds and adjudications, they will recommend a specific scope. While the committee working on this voted to keep the ten-year scope, they were informally reminded that this administration favors the seven-year scope, as illustrated in the revised SF-86. George Tenet personally favored seven years. One supporting argument is that no discernible advantage is gained (i.e., no more derogatory info is likely to be found) by adding three more years to investigative checks normally made. One counter-argument would be that seven years may not be enough to detect very undesirable traits or behaviors in candidates for clearances.

Ed Springer of OMB is pressing for an interim resolution, so that guidance to agencies for using the new SF-86 forms is consistent. My view is that a Presidential EO specifying 10 years can only be countermanded by another Presidential action. Alternative suggestions by OMB are SPB guidance, Tony Lake letter or other WH action, short of a new EO, PDD or POTUS memo, that would say use the seven-year scope until all the SPB criteria are confirmed.

Question: Is there any legal way (short of POTUS action) to reduce the scope from ten to seven years? Do you think we should initiate this action? (Comment: In reducing the scope of the SF-86, OMB did not address the old EO ten-year scope. That's not NSC's problem. However, agencies will logically look to us for guidance.)

→ Public notice
and comment
Time.

→

→ Form

MEMORANDUM FOR PETER SADERHOLM
Director, Security Policy Board Staff

SUBJECT: Guidelines and Standards Recommended by the
Security Policy Board, Per EO 12968

Thank you for the opportunity to suggest the appropriate mechanism for handling the SPB's recommendations to the President resulting from EO 12968, Access to Classified Information. Let me suggest an easy scenario, consistent with what we have discussed, and then some possible edits for the transmittal of the draft Adjudicative Guidelines for Clearances endorsed by the Security Policy Forum on July 28, 1995.

Simultaneous with SPB consideration of draft guidelines and standards (after SPF recommendation of the drafts to the SPB), I propose that you provide the drafts to me, and I will arrange their publication in the Federal Register, with a 14- to 30-day comment period. After the expiration of the comment period, the SPB can transmit the finalized draft to the National Security Affairs Advisor, noting that comments were (or were not) incorporated, based on the public notice. This strengthens the interagency and public support which Anthony Lake will have in recommending acceptance by the President.

As previously mentioned, some aspects of the guidelines and standards will be reviewed at the NSC and in the White House for conformance with the EO. Whether the President directs Mr. Lake to respond by memo or signs a memo himself, the drafts will be implemented by Presidential authority, as the EO sets out. I think that it is premature to suggest a new kind of directive, particularly in implementing a PDD that directs the SPB to recommend, and an EO that specifies the SPB will recommend, security policies to the President. The President has not yet delegated authority to direct security policies to the SPB. Of course, if the SPB decides to recommend some new form of directive to the President, and that the SPB be empowered to direct US Government-wide security policies, that is the SPB's prerogative. I suggest, however, that this may be premature.

You may also wish to review the notion that a PDD has too limited a circulation, or that some alternative White House document

could not just as easily do the job. The idea that we shouldn't bother the President with this level of detail is specifically invalidated by the wording in the EO.

I suggest you edit the Hall/Clark memo to read (p.1, 2.b.):

b. The Order requires the Board to submit its recommendations regarding the guidelines to the President through the Assistant to the President for National Security Affairs (APNSA). Based on discussions with NSC staff, we recommend that the draft be submitted to the NSC staff, who will arrange publication of the draft in the Federal Register, with a short deadline for response. Upon consideration of any comments and final edits, the Board would submit the guidelines to the NSC for approval. While the Order does not specify what form the documents will take, the NSC staff have indicated that the President, or the APNSA acting at the President's direction, will direct that the guidelines be put into effect in an appropriate White House document.

Regarding the Deutch/White draft memo, I suggest you may wish to edit paragraph #3. While there is nothing wrong with coining the term "Security Policy Directive," it would be inaccurate to omit NSC staff guidance, only mentioning Archives advice, and it may be premature to suggest that the SPB should issue directives on its own authority (not contained in PDD-29 or the EO).

I believe that after the implementing guidelines and standards required by EO 12968 are issued, there will be a number of issues the SPB will be addressing. In order to promulgate policy across the whole US Government, the SPB may be delegated authority to issue guidance on its own. It is the SPB's prerogative to recommend that to APNSA, the President or perhaps the Chief of Staff. However, I would suggest that you may wish to wait to do so until the basic documents called for in EO 12968 are finished and issued under the President's authority. At that point, there should be no political or administrative reasons why substantial opposition would be raised to those functions by the SPB.

Please let me know if this is or isn't helpful, or if I can be of further assistance on this or related issues.

Edward J. Appel
Director, Counterintelligence
Programs

*unclassified***FAX COVERSHEET****US SECURITY POLICY BOARD
(SPB) STAFF****1215 Jefferson Davis Highway, Suite 1101
Arlington, Virginia 22202**

TO: Ed Appel	FROM: Gary Harris
Office: NSC	Phone: (703) 602-7066
Phone: (202) 456-9341	Date: Sept 12, 1995
Fax: (202) 456-9340	Pages (incl. this cover sheet): 9
cc: Sandy Sagalkin	Phone: (703) 482-2689
Office: CMS	Fax: (703) 482-0684

Comments:

Ed,

This is the Adjudicative Guidelines package you discussed with Peter Saderholm. Notice the way we're proceeding: Forum co-chairs to forward the package to the Board co-chairs (3rd letter, attached); Board co-chairs in turn to circulate the Guidelines among the Board members (2nd letter, attached); assuming concurrence, Board co-chairs to forward the Guidelines to Natl Sec Advisor (top letter, attached). The letter to Dr. Lake advances the case for publishing the Guidelines as Security Policy Board Directives rather than as something more exalted, but leaves the final decision in his hands.

Gary

SPB UNCLASSIFIED FAX: (703) 602-7209**SPB CLASSIFIED FAX: (703) 602-6999****DSN: 322-xxxx***unclassified*

SECURITY POLICY BOARD

Arlington, Virginia 22202

MEMORANDUM FOR: The Honorable Anthony Lake
Assistant to the President for National
Security Affairs
National Security Council

FROM: The Honorable John M. Deutch
The Director of Central Intelligence

The Honorable John P. White
Cochairmen, Security Policy Board

SUBJECT: Adjudication Guidelines

1. This memorandum transmits to you, at Attachment A, the adjudication guidelines required by Section 3.2(b) of Executive Order 12968, Access to Classified Information. The Order directs us to forward them to the President through you for final approval.

2. The Order does not address how the guidelines are to be published. Presidential Decision Directive-29 created the Security Policy Board (Board) as a body to recommend to the President policy directives, legislative initiatives, and executive orders, but it also says nothing about how policy directives--in which category the adjudicative guidelines fit--should be promulgated. We believe that they should take the form of a Security Policy Directive, a new category of document that we propose issuing under the auspices of the Board, always subject, of course, to your review and approval. Because the guidelines help implement policy that the President has already approved with the signing of the Executive Order, they do not, in our judgment, warrant his attention. Furthermore, a Presidential Decision Directive's limited circulation would be incompatible with the need to have the guidelines in the hands of every adjudicator in the government. The Board Staff would coordinate distribution of Security Policy Directives at the agency level and their publication in the Federal Register. In the case of each new policy the Board proposes, you would be able to determine whether it should in fact appear as a Security Policy Directive or whether another type of document (Presidential Decision Directive, Executive Order) would be more appropriate. We believe this system has both practicality and efficiency on its side.

SUBJECT: Adjudication Guidelines

3. We accordingly recommend that you approve both the proposed guidelines and our preferred method for publication.

John M. Deutch

John P. White

Attachment

APPROVED:

Director of Central Intelligence

Date

Acting Deputy Assistant Secretary
of Defense (Intelligence and
Security)

Date

SECURITY POLICY BOARD

Arlington, Virginia 22202

MEMORANDUM FOR: Security Policy Board Members and Observers

FROM: The Honorable John M. Deutch
Director of Central IntelligenceThe Honorable John P. White
Deputy Secretary of Defense

SUBJECT: Adjudicative Guidelines

1. The Security Policy Forum has prepared for Security Policy Board (Board) action the Adjudicative Guidelines required by Executive Order 12968, Access to Classified Information.

2. Please review the Guidelines at Attachment A and respond to the Board Staff by 29 September 1995 with either your concurrence or your request to convene a meeting of the Board for discussion.

3. The Executive Order, while requiring us to forward the Guidelines to the President through his Assistant for National Security Affairs, does not specify how they should be published once approved. The Board Staff has been working with the National Archives and Records Administration and has concluded that they should take the form of a Security Policy Directive that would be published as a notice in the Federal Register. Attachment B is a draft cover memorandum to Dr. Lake that both forwards the Guidelines to him and recommends their publication as a Security Policy Directive.

John M. Deutch

John P. White

Attachments:

A. Adj Guidelines,
dtd 9 Jun 95

B. Draft Memo to Dr. Lake

Withdrawal/Redaction Marker

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001a. memo	For Security Policy Board members and observers. [partial] [CIA Act] (1 page)	09/12/1995	P3/b(3)

COLLECTION:

Clinton Presidential Records
National Security Council
Legal Advisor (Mary DeRosa)
OA/Box Number: 4058

FOLDER TITLE:

Personnel Security [9]

2006-1066-F

vz877

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]

SUBJECT: Adjudicative Guidelines

SPB/GHarris:dac:703/602-7066

Internal Distribution for SPB 159-95 (7 Sep 95):

Orig. - Security Policy Board Members

- 1 - The Honorable J. Deutch, CIA
- 1 - The Honorable J White, DepSecDef
- 1 - Mr. Paige, ASDC3I
- 1 - Mr. Slocombe, USD(P)
- 1 - Mr. Hall, ExDir/ICA

[001b]

P3/(b)(3)

- 1 - Mr. Clark, DASD(T&S)
- 1 - Lt Col Harris, SPBS
- 1 - SPB subj
- 1 - D/SPB chrono
- 1 - FTF
- 1 - DACF

Withdrawal/Redaction Marker

Clinton Library

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

001b. list	Addressees. [partial] [CIA Act] (1 page)	09/12/1995	P3/b(3)
------------	--	------------	---------

COLLECTION:

Clinton Presidential Records
National Security Council
Legal Advisor (Mary DeRosa)
OA/Box Number: 4058

FOLDER TITLE:

Personnel Security [9]

2006-1066-F

vz877

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]

SUBJECT: Adjudicative Guidelines

SPB/GHarris:dac:703/602-7066

Internal Distribution for SPB 159-95 (7 Sep 95):

Orig. - Security Policy Board Members

- 1 - The Honorable J. Deutch, CIA
- 1 - The Honorable J White, DepSecDef
- 1 - Mr. Paige, ASDCBI
- 1 - Mr. Slocombe, USD(P)
- 1 - Mr. Hall, ExDir/ICA

[001b]

P3(b)(3)

- 1 - Mr. Clark, DASD(T&S)
- 1 - Lt Col Harris, SPBS
- 1 - SPB subj
- 1 - D/SPB chrono
- 1 - FTF
- 1 - DACF

SPB 159-95/1
7 September 1995

MEMORANDUM FOR: The Honorable John M. Deutch
Director of Central Intelligence

The Honorable John P. White
Deputy Secretary of Defense

FROM: Keith R. Hall
Executive Director/Intelligence Community
Affairs

Jeremy C. Clark
Acting Deputy Assistant Secretary of Defense
(Intelligence and Security)

SUBJECT: Adjudicative Guidelines

1. Action Requested: That the Security Policy Board
cochairmen sign the attached memorandum.

2. Background:

a. Executive Order 12968, Access to Classified Information, tasks the Security Policy Board (Board) with developing common guidelines for making decisions regarding access eligibility. The Personnel Security Committee has prepared the adjudication guidelines, and the Security Policy Forum unanimously endorsed them on 28 July 1995. This memorandum forwards them to you for your review and for your signatures on the cover memorandum circulating them to the other members of the Board.

b. The Order requires the Board to submit its recommendations regarding the guidelines to the President through the Assistant to the President for National Security Affairs. Although it is clear that final approval is a Presidential prerogative, the Order does not specify the actual form the guidelines should take once approved. Furthermore, Presidential Decision Directive-29, which establishes the Board, instructs it to recommend policy directives, legislative initiatives, and executive orders to the President, but it also says nothing about how policy directives--in which category the adjudicative guidelines fit--should be published. We believe that they should be published as a Security Policy Directive, a new category of document that we

SUBJECT: Adjudicative Guidelines

propose issuing under the auspices of the Board. The guidelines help implement policy that the President has already approved with the signing of the Executive Order; thus, in our judgment, they do not warrant his attention. Furthermore, a Presidential Decision Directive's limited circulation would be incompatible with the need to have the guidelines in the hands of every adjudicator in the government. The Board Staff would coordinate distribution of Security Policy Directives at the agency level and coordinate their publication in the Federal Register. We believe this system has both practicality and efficiency on its side.

3. Recommendation: The attached package contains the cover memorandum to the Board members, the Adjudicative Guidelines, and a proposed memorandum to Dr. Anthony Lake. We recommend that you approve distribution of the package to your fellow Board members by signing the cover memorandum.

Keith R. Hall

Jeremy C. Clark

Attachment

SUBJECT: Adjudicative Guidelines

SPB/GHarris:dac:703/602-7066

Distribution of SPB 159-95/1 (7 Sep 95):

Orig. - The Honorable J. Deutch, CIA
- The Honorable J. White, DepSecDef
1 - Mr. Hall, ExDir/ICA
1 - Mr. Clark, A/DASD(I&S)
1 - Lt Col Harris, SPBS
1 - SPB subj
1 - D/SPB chrono
1 - FTF
1 - DACF

NATIONAL SECURITY COUNCIL

9/8

Jamie

I don't bother sending you early drafts, but this is nearly ready for prime time.

My only problems with it are a rather vague sentence, and the issue of definitions. There appears to be no intention to standardize definitions or deconflict the NISPM and DCID definitions.

Is this OK by you otherwise?

Ed Appel

To Jamie Baker
Legal

Withdrawal/Redaction Marker

Clinton Library

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

002. fax	Cover Sheet. List of Addressees. [partial] [CIA Act] [10 U.S.C. §424] [National Security Act] (1 page)	08/18/1995	P3/b(3)
----------	---	------------	---------

COLLECTION:

Clinton Presidential Records
National Security Council
Legal Advisor (Mary DeRosa)
OA/Box Number: 4058

FOLDER TITLE:

Personnel Security [9]

2006-1066-F
vz877

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]

UNCLASSIFIED**FAX COVER SHEET**

U.S. SECURITY POLICY BOARD STAFF
1215 Jefferson Davis Highway, Suite 1101
Arlington, VA 22202

FROM: DICK WEAVER PHONE: 703/602-7215 DATE: 18 August 1995

TO: POLICY INTEGRATION COMMITTEE MEMBERS

<u>DEPARTMENT/AGENCY</u>	<u>MEMBER</u>	<u>FAX NUMBER</u>
DOE	Dave Jones	301/903-8717
Coast Guard	Ron Seidman	202/267-4949
OUSDP	Dr. Lin Wells	703/614-8976
OASD-C ³ I	Rene Davis-Harding	703/695-8215
NASA	Mark Borsi	202/358-3238
JCS	Harry Guerrier	703/614-5059
FEMA	Larry Berenson	202/646-3155
Army	Col Richard Demers	703/614-6885
P3/(b)(3)		
Navy	Mike Brown	202/433-8849
Marines	LtCol Dandridge Carter	703/614-6250
Air Force	Gene Bocsch	703/693-2059
State	Robert Spencer	202/663-0678
P3/(b)(3)		
FBI	Robert Opier	202/324-8524
Justice	Jerry Rubino	202/514-4555
Commerce	Steve Gannon	202/482-0183
Treasury	Rick Riley	202/622-1056
ISOO	Dr. Ethel Theis	202/395-7460
OPM	Richard Ferris	202/376-3840
Transportation	John Taylor	202/366-7013
OMB	Paul Brower	202/456-0752
NRC	Ray Brady	301/415-5132
DISA	Rob Rogalski	703/607-4194
GSA	Joe Rodriguez	202/208-5430
P3/(b)(3)		
NSC	Ed Appel	202/456-9340
CMS	Sandy Sagalkin	703/482-0684
Industry (Observer)	Harry Volz	516/541-5517
P3/(b)(3)		

[002]

COMMENTS: Attached is the draft reciprocity policy for next Friday's meeting (25 August 1995 from 1000-1200).

SPB FAX (U): 703-602-7219/ SPB FAX (S) (STU-III) FAX: 703-602-5892
 (Coord on: 703/602-6997) DSN PREFIX: 332-XXXX

TOTAL # OF PAGES: ____ (INCLUDING COVER SHEET)

UNCLASSIFIED

TOPIC**RECIPROCITY OF CLEARED FACILITIES**Action Required:

Approve Policy Directive on Reciprocity of cleared facilities for forwarding to the Security Policy Forum.

Background:

In two separate recommendations (#44 and #46), the Joint Security Commission recommended reciprocity of accreditations and inspections of facilities; aperiodic, random inspections conducted no more frequently than annually, and creation of a database to register certified facilities. On 24 April 1995, the Security Policy Board combined these recommendations into a single recommendation, approved the policy, and tasked the Facilities Protection Committee to develop a plan to implement this recommendation, including a data base for registering certified facilities and reciprocity of inspections/reviews, and report back to the Security Policy Board within three months.

The Facilities Protection Committee developed a Policy Directive which requires all government organizations to accept the approval, certification, or accreditation of a facility at the same security level without change, enhancements or upgrades. It also requires government organizations to conduct security reviews no more frequently than annually. Additionally, security reviews will be aperiodic or random, be announced, and be based upon risk management principles. Agencies will continue to review and assess the value added to the process of co-use of facilities by development of electronic data retrieval across government. Until an electronic data retrieval system is developed, the Security Policy Board Staff will maintain a list of agency personnel to be contacted for verification of approved, certified, or accredited facility status. As this review continues, agencies creating or modifying facility databases are required to do so in a manner which facilitates community data sharing. Agencies are required to develop internal procedures to implement this policy effective 1 December 1995. A set of approved terms and guiding principles was attached for use in development of agency procedures. Since the Facilities Protection Committee unanimously recommended approval of the attached policy, definitions, and guiding principles, it was placed on the Forum agenda at their 28 July meeting.

Two agencies dissented at the Forum - Department of Energy wanted the capability to conduct unannounced inspections and to have it vetted through the Policy Integration Committee. The Nuclear Regulatory Commission also dissented and requested the PIC look at it. The Forum Co-chairs and SPB Staff Director assigned it to a small PIC working group to polish up the language.

The PIC WG met and decided to delete the definitions and the guiding principles and came up with a one page plan vice policy for reciprocity. Upon staffing, several agencies reiterated the need for common definitions and a strong policy statement. The SPB Staff incorporated these comments and drafted Attachment A. It consists of a policy, glossary, and implementation plan. In addition to the features cited above, this version of the policy allows for unannounced inspections if conducted "for cause". It allows those agencies who wish to use a rating system for inspections to do so and standardizes the definition of each rating. It adds the term inspection vice security review because many agencies (all those governed by the DCI Directives) conduct inspections instead of reviews. Several terms defined in the glossary are different than those found in the NISPOM or DCIDs. This was necessary because the previous definitions applied only to that particular document's audience (i.e. industry for the NISPOM and the compartmented community for the DCIDs). Per previous SPF decision, this policy is intended to apply across the board to both government and industry facilities at all security levels. To avoid confusion between the NISPOM, DCIDs or other predecessor documents, the glossary contains a statement the definitions apply only to this policy and are not intended to contradict other previously defined terms.

DECISION OPTIONS:

_____ Approve the draft as written and recommend it be forwarded to the Forum.

_____ Change the draft as follows and forward to the Forum:

_____ Disapprove the draft and recommend it be returned to the Facilities Protection Committee for additional work and staffing.

DRAFT

**SECURITY POLICY BOARD
POLICY
ON RECIPROCITY OF
ACCREDITATIONS AND INSPECTIONS/REVIEWS
OF FACILITIES**

It is the policy of the United States Government ¹ that once a government or industrial facility is approved, certified, or accredited to safeguard classified material, all government organizations desiring to conduct security programs at the facility at the same, or lower security level shall accept the approval, certification, or accreditation without change, enhancements, or upgrades. ²

After initial security approval, certification, or accreditation, subsequent security reviews/inspections shall be based on risk management principles, be aperiodic, normally be conducted no more frequently than annually, and be announced. Additionally, as demanded by risk management principles (which includes analysis of the value of the classified assets at the facility, the threats to the facility, the vulnerability of the facility, and the effectiveness of the established countermeasures), security reviews/inspections may be conducted "for cause", to follow up on previous findings, or to accomplish close-out actions. Security reviews/inspections conducted for cause may be unannounced.

Each security review/inspection must ensure the inspected facility maintains a security program that safeguards classified information. Any security review/inspection results that may impact the approval, certification, or accreditation status of a facility will be shared with the Cognizant Security Authorities/Agencies/Offices (CSAAO) co-using that facility. The CSAAO has the responsibility to notify other CSAAO co-utilizing the facility of any changes to the security posture of a facility. Joint security reviews between CSAAO co-using the facility are encouraged. The CSAAO shall coordinate the termination of the Facility Security Clearance/accreditation with other agencies that are co-utilizing the space.

Although not required, some Agencies may elect to use ratings for each security review/inspection. These ratings, if used, cannot affect reciprocity and shall meet the standards cited in the Glossary.

¹ At its 24 April 1995 meeting, the Security Policy Board approved a policy of reciprocity of accreditation and inspection of both government and industrial facilities. For industry, the National Industrial Security Program Operating Manual (NISPOM) states that "a facility clearance shall be considered valid and acceptable for use on a fully reciprocal basis by all Federal departments and agencies, provided it meets or exceeds the level of clearance needed".

² This reciprocity is being achieved through the NISPOM, the NISPOM Supplement, the Director of Central Intelligence Directives, interagency agreements, or other mutually agreed upon methods.

DRAFT

Visits (non security reviews/inspections) may be made to a facility to conduct security support actions, administrative inquiries, program reviews, and approvals. Reasons for, and the results of such visits by one agency cannot, in any way, affect the facility security clearance/accreditation, or reciprocity agreements of that facility unless coordinated with and agreed to by the CSAOs of all affected government organizations. }

?

CSAOs will share facility security clearance/accreditation information on a need-to-know basis. Data sharing currently exists within each of the collateral, SAP, and SCI communities through points of contact representing each CSAO. Facility representatives provide identification of the approving/accrediting organization to the potential co-user and the co-user interacts with the accrediting organization to formalize the arrangement.

Agencies which approve, certify, or accredit facilities shall provide to the Security Policy Board Staff by October 1, 1995 the names and telephone numbers of personnel to be contacted for verification of approved, certified, or accredited facility status. Where unclassified dial-in capability exists, this information shall also be provided. The Security Policy Board Staff will publish and update as necessary a comprehensive directory of these points of contact by November 1, 1995.

Annexes:

- A. Glossary
- B. Implementation Plan

DRAFT**ANNEX A****GLOSSARY**

NOTE: The definitions cited below are provided to assist in the implementation of this basic policy. They are not intended to contradict or replace definitions in predecessor policies (i.e. NISPOM, Director of Central Intelligence Directives, etc.). They only apply to this policy.

ACCREDITATION: The formal approval of a specific place, building, room, group of rooms, or defined space that meets prescribed physical, technical, and personnel security standards. {applies to SCI and SAP programs}

COGNIZANT SECURITY AGENCY: Agencies of the Executive Branch that have been authorized to establish a security program for the purpose of safeguarding classified information held by a federal government organization or its contractors.

COGNIZANT SECURITY AUTHORITY: The responsible agency of the Executive Branch that has jurisdiction over specific classified information. (i.e. the DCI is the Cognizant Security Authority for intelligence sources and methods; the DoE and NRC are the Cognizant Security Authorities for Restricted Data and Formerly Restricted Data).

COGNIZANT SECURITY OFFICE: The office or offices delegated by the Head of a Cognizant Security Agency or Authority to administer security in a facility on behalf of the Cognizant Security Agency or Authority.

CO-USE/CO-UTILIZATION: Two or more governmental organizations or programs sharing the same approved/accredited space.

FACILITY: A specific physical space that has been formally approved/accredited in writing which satisfies the criteria for generating, safeguarding, handling, discussing, and storing of classified and/or unclassified program information.

FACILITY SECURITY CLEARANCE: An administrative determination that a facility is eligible for access to information at a specific classification level (and all lower levels).

FOR CAUSE REVIEW/INSPECTION: A review/inspection in response to actual or potential violation of statute, regulation, manual, directive, or contractual obligation.

DRAFT

PROGRAM REVIEW: Multi disciplinary technical reviews for contractual purposes by government personnel which may include a security element; with this security element providing consultation and problem-solving, not for security review purposes.

RATINGS: (Not required)

Superior: An outstanding security program reflecting no system failures; widespread knowledge among cleared employees of security regulations and procedures; demonstrated support by all levels of management.

Satisfactory: Program/Activity being evaluated meets protection objectives.

Marginal: Program/Activity being evaluated only partially meets protection objectives.

Unsatisfactory: Program/Activity being evaluated does not meet protection objectives.

RECIPROCITY: Agreement between Cognizant Security Authority/Agency/Office to accept security related determinations concerning facilities, program areas and program operations made by another Cognizant Security Authority/Agency/Office, when operating at the same security level.

SECURITY REVIEW/INSPECTION: A process (1) to determine the organization's continued eligibility for a facility security clearance or accreditation; (2) to ensure that the organization has developed and implemented a program to provide adequate protection; and (3) to terminate a facility security clearance.

DRAFT**ANNEX B****IMPLEMENTATION PLAN**

1. Security Policy Board publish this policy.
2. Continue actions already underway, including:
 - a. Memoranda of Agreement between Executive Branch agencies are a prerequisite to reciprocity. Several Executive Branch agencies have already entered into Memoranda of Agreement. Other agencies are currently in the process of drafting or negotiating agreements.
 - b. Standardization of facility security clearances and accreditations is a key to reciprocity. Standardization of facility security clearances and accreditations is prescribed by the NISPOM and DCID 1/21.
 - c. Databases on both facility clearances and personnel security clearances must be shared. Data sharing currently exists within each of the collateral, SAP, and SCI communities through points of contact representing each Cognizant Security Authority/Agency/Office. The collateral, SAP, and SCI communities will, as time and budget resources permit, continue to work towards electronic data retrieval, first within the individual communities then across the communities. Agencies are working together to establish commonality of facility databases. As an interim measure, the Security Policy Board will maintain a list of agency points of contact.
 - d. Standardized training is a key to reciprocity. Standardized training is being addressed by government and industry entities.
 - e. Standardization of forms for government and industry are currently being developed. When complete, the draft forms will be coordinated among the Executive Branch agencies.
3. Through the Facilities Protection Committee, agencies will continue to review and assess the potential utility of a database in the process of co-use. As this review continues, agencies creating or modifying facilities databases will do so in a manner which facilitates community data sharing.

NATIONAL SECURITY COUNCIL

September 8, 1995

To: Jamie Baker (348)

From: Ed Appel

Please provide your
comments/clearance by COB
today.

thanks

Action

September 8, 1995

ACTION

MEMORANDUM FOR ANTHONY LAKE

THROUGH: R. RAND BEERS

2 issues

FROM: EDWARD J. APPEL

SUBJECT: Draft Executive Order on Interagency Security
CommitteeBackground

After the April 19, 1995 bombing of the Oklahoma City federal building, the President ordered a study, titled "Vulnerability Assessment of Federal Buildings," which was published June 28, 1995. Among other recommendations, the report stated, under "4.2.5 Create An Interagency Security Committee:" "To provide a permanent body to address continuing government-wide security concerns, an Interagency Security Committee (ISC) should be created by Executive Order. Federal Protective Service (FPS) should be authorized to chair and staff the ISC and be responsible for implementing and monitoring any ISC recommendations. Membership should include permanent representation by the USMS, GSA and each cabinet-level agency currently on the President's Management Council..." (The Assistant Commissioner, FPS, reports to the Commissioner, Public Buildings Service, GSA.) The President accepted the recommendations in the report.

*who did
read*

OMB is circulating a "fast track" draft Executive Order, which would provide for a new Interagency Security Committee, chaired by the Assistant Commissioner, FPS, with representatives from most US departments and agencies. Based on comments from the staff of the Security Policy Board and NSC, OMB proposed inclusion of the SPB Staff Director on the Committee and accepted my suggestion to designate the GSA Administrator, rather than FPS Assistant Commissioner, as Committee chairman. Roger Johnson, GSA Administrator, indicated that he wishes to discuss NSC's rationale in selecting him versus the FPS head as chair. GSA is

agreed

in a more powerful position to bring about rapid upgrading of federal buildings' security, has more credibility than FPS and oversees broader security policies for the federal workplace than FPS handles. Further, FPS may suffer from some credibility problems as chair of an interagency committee with a dynamic charter.

As you are aware, President Clinton signed Presidential Decision Directive-29 in September, 1994, establishing the Security Policy Board (DCI and Dep Sec Def Co-Chairs, with Dep Sec State, Vice Chairman, JCS, Under Sec Energy, Dep Sec Commerce, Dep AG, one Dep Sec from Non-Defense Agency, OMB and NSC members); its subordinate Security Policy Forum (26 federal agencies) and its five standing committees, including a Facilities Protection Committee. This structure (for the first time) unifies, standardizes and brings the combined expertise of the executive branch together to address security issues. While routine civilian federal building security was not considered a pressing issue until April 19th, the Facilities Protection Committee demonstrated its functionality and capabilities by addressing a knotty old issue, reciprocity for facilities clearances, in an efficient manner.

Comments

Since the SPB is up and running well, has a staff and interagency infrastructure and has credible expertise in all aspects of security, it is a better choice to take on buildings security improvement than a new, independent committee. Duplication of effort (with attendees committed to two committees) would be avoided.

As a response to potential federal buildings vulnerabilities, designation of FPS to chair a new interagency group lacks credibility. A higher level chair should be chosen. The GSA Administrator would be a better choice. However, GSA is not responsible for all government facilities, nor do they have the infrastructure or overall security expertise to lead the US effort rapidly to upgrade building security overall without help. A better alternative would be to instruct the Security Policy Board to direct the Facilities Protection Committee to undertake the mission outlined in the Vulnerability Assessment, organize the interagency committee to do so and meet several specific requirements which the President or you could direct.

Concurrence by: Richard Clarke Steve Simon James Baker

RECOMMENDATIONS

1. That the GSA Administrator be chosen to chair the new Interagency Security Committee (rather than the Assistant Commissioner of FPS), if such a committee is to be created by Executive Order.

Approve _____ Disapprove _____

2. That in lieu of creating a new Interagency Security Committee, the Security Policy Board be instructed to utilize its existing Facilities Protection Committee (to include GSA and FPS) to address prompt upgrading of federal buildings. You could elect to do so, or the President, by Executive Order or memorandum could do so.

Approve _____ Disapprove _____

Attachment

Tab I Draft Executive Order

I

EXECUTIVE ORDER

INTERAGENCY SECURITY COMMITTEE

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by federal employees for non-military activities ("federal facilities"), and to provide a permanent body to address continuing government-wide security for Federal facilities, it is hereby ordered as follows:

Section 1. Interagency Security Committee. (a) Establishment. There is hereby established within the Executive Branch an Interagency Security Committee (the "Committee").

(b) Membership. The Committee shall consist of representatives from the following agencies, appointed by the agency heads, and other individuals or their designees:

- (i) Department of State;
- (ii) Department of the Treasury;
- (iii) Department of Defense;
- (iv) Department of Justice;
- (v) Department of the Interior;
- (vi) Department of Agriculture;
- (vii) Department of Commerce;
- (viii) Department of Labor;
- (ix) Department of Health and Human Services;
- (x) Department of Housing and Urban Development;
- (xi) Department of Transportation;
- (xii) Department of Energy;
- (xiii) Department of Education;
- (xiv) Department of Veterans Affairs;
- (xv) Environmental Protection Agency;
- (xvi) Central Intelligence Agency;
- (xvii) Office of Management and Budget;
- (xviii) General Services Administration;

- (xix) The Director of the United States Marshals Service;
- (xx) The Assistant Commissioner of the Federal Protective Service of the Public Buildings Service, United States General Services Administration;
- (xxi) The Assistant to the President for National Security Affairs;
- (xxii) The Director of the Security Policy Board; and
- (xxiii) such other Federal employee members as the President shall appoint.

(c) Chair. The Committee shall be chaired by the Assistant Commissioner of the Federal Protective Service of the United States General Services Administration ("Assistant Commissioner"), or the designee of the Assistant Commissioner.

(d) Working Group. The Committee is authorized to established interagency working groups to perform such task as may be directed by the Committee.

Sec. 2. Duties and Responsibilities. (a) The Committee shall: (i) Establish policies for security in and protection of Federal facilities.

(ii) Develop and evaluate security standards for Federal facilities; develop a strategy for ensuring compliance with such standards; and oversee the implementation of appropriate security measures in Federal facilities; and

(iii) Take such actions as may be necessary to enhance the quality and effectiveness of security and protection of Federal facilities, including but not limited to:

- a. encouraging agencies with security responsibilities to share security-related intelligence in a timely and cooperative manner;
- b. assessing technology and information systems as a means of providing cost-effective improvements to security in Federal facilities;

- c. developing long term construction standards for those locations with threat levels or missions that require blast resistant structures or other specialized security requirements;
- d. evaluating standards for the location of, and special security related to, day care centers in Federal facilities; and
- e. assisting the Administrator of General Services in developing and maintaining a centralized security data base of all Federal facilities.

Sec. 3. Agency Support and Cooperation. (a) Administrative Support. To the extent permitted by law and subject to the availability of appropriations, the Administrator of General Services, acting by and through the Assistant Commissioner, shall provide the Committee such administrative services, funds, facilities, staff and other support services as may be necessary for the performance of its functions under this Order.

(b) Cooperation. Each executive agency and department shall cooperate and comply with the policies and recommendations of the Committee issued pursuant to this Order, except where the Director of Central Intelligence determines that compliance would jeopardize intelligence sources and methods. To the extent permitted by law and subject to the availability of appropriations, executive agencies and departments shall provide such support as may be necessary to enable the Committee to carry out its duties and responsibilities under this Order.

(c) Compliance. The Administrator of General Services, acting by and through the Assistant Commissioner, shall be responsible for implementing and monitoring Federal agency compliance with committee policies and recommendations.

Sec. 4. Judicial Review. This order is intended only to improve the internal management of the Federal government, and is not intended to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its officers or any person.

Sec. 5. Effective Date. This Order shall be effective immediately.

THE WHITE HOUSE,

Ed,

9-13-95

Roger Johnson has agreed to chair the
Interagency Security Committee. I plan to
go forward with the processing now.

Thank you for your help on this matter.

Woe (x53563)

- - - - -

INTERAGENCY SECURITY COMMITTEE

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by federal employees for non-military activities ("federal facilities"), and to provide a permanent body to address continuing government-wide security for Federal facilities, it is hereby ordered as follows:

Section 1. Interagency Security Committee. (a) Establishment. There is hereby established within the Executive Branch an Interagency Security Committee (the "Committee").

(b) Membership. The Committee shall consist of representatives from the following agencies, appointed by the agency heads, and other individuals or their designees:

- (i) Department of State;
- (ii) Department of the Treasury;
- (iii) Department of Defense;
- (iv) Department of Justice;
- (v) Department of the Interior;
- (vi) Department of Agriculture;
- (vii) Department of Commerce;
- (viii) Department of Labor;
- (ix) Department of Health and Human Services;
- (x) Department of Housing and Urban Development;
- (xi) Department of Transportation;
- (xii) Department of Energy;
- (xiii) Department of Education;
- (xiv) Department of Veterans Affairs;
- (xv) Environmental Protection Agency;
- (xvi) Central Intelligence Agency;
- (xvii) Office of Management and Budget;
- (xviii) General Services Administration;

- (xix) The Director of the United States Marshals Service;
- (xx) The Assistant Commissioner of the Federal Protective Service of the Public Buildings Service, United States General Services Administration ("Assistant Commissioner");
- (xxi) The Assistant to the President for National Security Affairs;
- (xxii) The Director of the Security Policy Board; and
- (xxiii) such other Federal employee members as the President shall appoint.

(c) Chair. The Committee shall be chaired by the Administrator of General Services ("Administrator"), or the designee of the Administrator.

(d) Working Group. The Committee is authorized to establish interagency working groups to perform such tasks as may be directed by the Committee.

Sec. 2. Duties and Responsibilities. (a) The Committee shall: (i) Establish policies for security in and protection of Federal facilities.

(ii) Develop and evaluate security standards for Federal facilities; develop a strategy for ensuring compliance with such standards; and oversee the implementation of appropriate security measures in Federal facilities; and

(iii) Take such actions as may be necessary to enhance the quality and effectiveness of security and protection of Federal facilities, including but not limited to:

- a. encouraging agencies with security responsibilities to share security-related intelligence in a timely and cooperative manner;
- b. assessing technology and information systems as a means of providing cost-effective improvements to security in Federal facilities;
- c. developing long term construction standards for those locations with threat levels or missions that require

blast resistant structures or other specialized security requirements;

- d. evaluating standards for the location of, and special security related to, day care centers in Federal facilities; and
- e. assisting the Administrator in developing and maintaining a centralized security data base of all Federal facilities.

Sec. 3. Agency Support and Cooperation. (a) Administrative Support. To the extent permitted by law and subject to the availability of appropriations, the Administrator, acting by and through the Assistant Commissioner, shall provide the Committee such administrative services, funds, facilities, staff and other support services as may be necessary for the performance of its functions under this Order.

(b) Cooperation. Each executive agency and department shall cooperate and comply with the policies and recommendations of the Committee issued pursuant to this Order, except where the Director of Central Intelligence determines that compliance would jeopardize intelligence sources and methods. To the extent permitted by law and subject to the availability of appropriations, executive agencies and departments shall provide such support as may be necessary to enable the Committee to carry out its duties and responsibilities under this Order.

(c) Compliance. The Administrator, acting by and through the Assistant Commissioner, shall be responsible for monitoring Federal agency compliance with committee policies and recommendations.

Sec. 4. Judicial Review. This order is intended only to improve the internal management of the Federal government, and is not intended to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its officers or any person.