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:				
Personnel Security [5]				
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. letter	To Stephen Preston from CIA Counsel. [partial] [CIA Act] (1 page)	11/18/1997	P3/b(3)
001b. memo	For Various from Stephen Preston. [partial] [CIA Act] (1 page)	11/05/1997	P3/b(3)
002. memo	For Alan Kreczko from Charles Ruff. Subject: Clearances. (1 page)	04/08/1997	P6/b(6)
003a. memo	For James Hall from Glyn Davies. Subject: Anthony Lake's Clearance Certification. [partial] (1 page)	04/22/1997	P6/b(6)
003b. draft	For James Hall from Glyn Davies. Subject: Anthony Lake's Clearance Certification. [partial] (1 page)	04/22/1997	P6/b(6)
004. memo	Duplicate of 003a. (1 page)	04/22/1997	P6/b(6)

COLLECTION:

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

FOLDER TITLE:

Personnel Security [5]

2006-1066-F
vz874

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]**

February 28, 1997

Directive on Safeguarding Classified National Security Information

[Effective Date]

Authority

This Directive is issued pursuant to Section 5.2 (c) of Executive Order (E.O.) 12958, "Classified National Security Information." The E.O. and this Directive set forth the requirements for the safeguarding of classified national security information (hereinafter classified information) and are applicable to all U.S. Government Agencies.

Section I - General

(a) Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification.

(b) Except for NATO and other foreign government information, agency heads or their designee(s) (hereinafter referred to as agency heads) may adopt alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements. When the use of alternative measures are other than situational, the alternative measures shall be documented and provided to the Director, Information Security Oversight Office (ISOO), to facilitate that office's oversight responsibility. Upon request, the description shall be provided to any other agency with which classified information or secure facilities are shared. In all cases, the alternative measures shall provide protection sufficient to reasonably deter and detect loss or unauthorized disclosure. Risk management factors considered will include criticality, sensitivity, and value of the information; analysis of known and anticipated threats; vulnerability; and countermeasures benefits vs. cost.

(c) NATO classified information shall be safeguarded in compliance with U.S. Security Authority for NATO Instructions I-69 and I-70. Other foreign government information shall be safeguarded as described herein for U.S. information except as required by an existing treaty, agreement or other obligation (hereinafter, obligation).

Atch B

When the information is to be safeguarded pursuant to an existing obligation, the additional requirements at Annex B may apply to the extent they were required in the obligation as originally negotiated or are agreed upon during amendment. Negotiations on new obligations or amendments to existing obligations shall strive to bring provisions for safeguarding foreign government information into accord with standards for safeguarding U.S. information as described in this Directive.

(d) An agency head who originates or handles classified information shall refer any matter pertaining to the implementation of this Directive that he or she cannot resolve to the Director, ISOO for resolution.

Section II - Definitions

(a) Open Storage Area: An area, constructed in accordance with Annex A and authorized by the agency head for open storage of classified information.

(b) Authorized Person: A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know for the specific classified information in the performance of official duties.

(c) Cleared Commercial Carrier: A carrier that is authorized by law, regulatory body, or regulation, to transport SECRET and CONFIDENTIAL material and has been granted a SECRET facility clearance in accordance with the National Industrial Security Program.

(d) Security-in-Depth: A determination by the agency head that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed open storage areas, and security storage cabinets during non-working hours.

(e) Vault: An area approved by the agency head which is designed and constructed of masonry units or steel lined construction to provide protection against forced entry. A GSA-approved modular vault may be used in lieu of the above. Vaults shall be equipped with a GSA-approved vault door and lock.

Section III - Responsibilities of Holders

Authorized persons having access to classified information are responsible for: (a) protecting it from persons not authorized access to it, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person; (b) meeting safeguarding requirements prescribed by the agency head; and (c) ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

Section IV - Standards for Security Equipment

The Administrator of General Services shall, in coordination with agency heads originating classified information, establish and publish uniform standards, specifications and supply schedules for security equipment designed to provide secure storage for and destruction of classified information. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above, and shall, to the maximum extent possible, be of the type available through the Federal Supply System.

Section V - Storage

(a) General. Classified information shall be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government controlled facilities unless otherwise stipulated in treaties or international agreements. Overseas storage standards for facilities under a Chief of Mission are promulgated under the authority of the Overseas Security Policy Board.

(b) Requirements for Physical Protection:

(1) **Top Secret.** Top Secret information shall be stored by one of the following methods:

(A) In a GSA-approved security container with one of the following supplemental controls:

(i) The location that houses the security container shall be subject to continuous protection by cleared guard or duty personnel;

(ii) Cleared guard or duty personnel shall inspect the security container once every two hours;

(iii) An Intrusion Detection System[1] (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; or

(iv) Security-In-Depth when the GSA-Approved container is equipped with a lock meeting Federal Specification FF-L-2740.

<u>OR</u>

(B) In either of the following: (i) An open storage area constructed in accordance with Annex A, which is equipped with an IDS with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth or a five minute alarm response if it is not; or (ii) an IDS-equipped vault with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(2) **Secret**. Secret information shall be stored by one of the following methods:

(A) In the same manner as prescribed for Top Secret information;

(B) In a GSA-approved security container or vault without supplemental controls; or

(C) In either of the following: (i) Until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA approved container secured with a rigid metal lockbar and an agency head approved padlock;[2] or (ii) An open storage area. One of the following supplemental controls is required:

(i) The location that houses the container or open storage area shall be subject to continuous protection by cleared guard or duty personnel;

(ii) Cleared guard or duty personnel shall inspect the security container or open storage area once every four hours; or

(iii) An IDS (per footnote 1) with the personnel responding to the alarm arriving within 30 minutes

---

[1] "Acceptability of Intrusion Detection Equipment (IDE): All IDE must be UL-listed (or equivalent as defined by the agency head) and approved by the agency head. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head."

[2] Security-in-depth as determined by the agency head is required, in addition to V(b)(2)(C)(i)(ii) or (iii) above, as part of the supplemental controls for a non-GSA approved container storing Secret information.

of the alarm annunciation;

(3) **Confidential.** Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

(c) Combinations. Description: Dial-type locks; and other changeable combination locks.

(1) Equipment in service. The classification of the combination shall be the same as the highest level of classified information that is protected by the lock. Combinations to dial-type locks shall be changed only by persons having a favorable determination of eligibility for access to classified information and authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination. Combinations shall be changed under the following conditions:

(A) Whenever such equipment is placed into use;

(B) whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or

(C) whenever a combination has been subject to possible unauthorized disclosure.

(2) Equipment out of service. When security equipment is taken out of service, it shall be inspected to ensure that no classified information remains and the built-in combination lock shall be reset to a standard combination.

(d) Key Operated Locks. When special circumstances exist, an agency head may approve the use of key operated locks for the storage of Secret and Confidential information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be established.

Section VI - Information Controls

(a) General. Agency heads shall establish a system of control measures which assure that access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which the access occurs and the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures which may include records of internal distribution, access, generation, inventory, reproduction, and disposition shall be required when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized persons.

(b) Reproduction. Reproduction of classified information shall be held to the minimum consistent with operational requirements. The following additional control measures shall be taken:

(1) Reproduction shall be accomplished by authorized persons knowledgeable of the procedures for classified reproduction;

(2) unless restricted by the originating Agency, Top Secret, Secret, and Confidential information may be reproduced to the extent required by operational needs, or to facilitate review for declassification;

(3) copies of classified information shall be subject to the same controls as the original information; and

(4) the use of technology that prevents, discourages, or detects the unauthorized reproduction of classified information is encouraged.

Section VII - Transmission

(a) General. Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Directive.

(b) Dispatch. Agency heads shall establish procedures which ensure that:

(1) All classified information physically transmitted outside facilities shall be enclosed in two layers; both of which provide reasonable evidence of tampering and which conceal the contents. The inner enclosure shall clearly identify the address of both the sender and the intended recipient, the highest classification level of the contents, and any appropriate warning notices. The outer enclosure shall be the same except that no markings to indicate that the contents are classified shall be visible. Intended recipients shall be identified by name only as part of an attention line. The following exceptions apply:

(A) If the classified information is an internal component of a packageable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information;

(B) if the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered to be a sufficient enclosure provided observation of it does not reveal classified information;

(C) if the classified information is an item of equipment that is not reasonably packageable and the shell or body is classified, it shall be concealed with an opaque enclosure that will hide all classified features;

(D) specialized shipping containers, including closed cargo transporters or diplomatic pouch, may be considered the outer enclosure when used; and

(E) when classified information is hand-carried outside a facility, a locked briefcase may serve as the outer enclosure.

(2) Couriers and authorized persons designated to hand-carry classified information shall ensure that the information remains under their constant and continuous protection and that direct point-to-point delivery is made. As an exception, agency heads may approve the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, secured with a high security padlock and equipped with an electronic seal that would provide evidence of surreptitious entry, as a substitute for a courier on direct flights provided that arrangements are made to ensure that the carrier protects the container until its delivery is completed.

(c) <u>Transmission methods within and between the U.S., Puerto Rico, or a U.S. possession or trust territory</u>.

(1) **Top Secret** information shall be transmitted by: direct contact between authorized persons; the Defense Courier Service or an authorized government agency courier service; a designated courier or escort cleared Top Secret; electronic means over approved communications systems. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service.

(2) **Secret** information shall be transmitted by:

(A) any of the methods established for Top Secret; U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail; and cleared commercial carriers or cleared commercial messenger services. (Note: The Waiver of Signature and Indemnity block, item 11-B, on the U.S. Postal

Service Express Mail Label shall not be completed. The use of street-side mail collection boxes is strictly prohibited.); and

(B) on an exceptional basis when applicable postal regulations (39 C.F.R.) are met agency heads may, when an urgent requirement exists for overnight delivery within the U.S. and its Territories, authorize the use of the current holder of the General Services Administration contract for overnight delivery of information for the Executive Branch. Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The contract shall require cooperation with government inquiries in the event of a loss, theft, or possible unauthorized disclosure of classified information. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the correct mailing address. The package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified Communications Security Information, NATO, and foreign government information shall not be transmitted in this manner.

(3) **Confidential** information shall be transmitted by any of the methods established for Secret information or U.S. Postal Service Certified Mail. In addition, U.S. First Class Mail may be used as a means of transmission, when the recipient is a U.S. Government facility. Confidential information shall not be transmitted to government contractors via first class mail. When first class mail is used, the envelope or outer wrapper shall be marked to indicate that the information is not to be forwarded but is to be returned to sender. The use of street-side mail collection boxes is prohibited.

(d) Transmission methods to a U.S. Government facility located outside the U.S. The transmission of classified information to a U.S. Government facility located outside the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession or trust territory, shall be by methods specified above for Top Secret information or by the Department of State Courier Service. U.S. Registered Mail through Military Postal Service facilities may be used to transmit Secret and Confidential information provided that the information does not at any time pass out of U.S. citizen control nor pass through a foreign postal system.

(e) Transmission of U.S. classified information to foreign governments. Such transmission shall take place between designated government representatives using the transmission methods described above. When classified information is transferred to a foreign government or its representative, a signed receipt is required.

(f) Receipt. Agency heads shall establish procedures which ensure that classified information is received in a manner which precludes unauthorized access, provide for inspection of all classified information received for evidence of tampering and confirmation of contents, and ensure timely acknowledgment of the receipt of Top Secret and Secret information by an authorized recipient. (Note, a receipt acknowledgment of all classified material transmitted to a foreign government or its representative, including its contractors is required).

Section VIII - Destruction

(a) General. Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by agency heads. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing.

(b) Technical guidance. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media, processing equipment components, and the like may be obtained by submitting all pertinent information to NSA/CSS Directorate for Information Systems Security, Fort Meade, MD 20755. Specifications concerning appropriate equipment and standards for the destruction of other storage media may be obtained from the General Services Administration.

Section IX - Loss, Possible Compromise or Unauthorized Disclosure

(a) General. Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) shall immediately report the circumstances to an official designated for this purpose.

(b) Cases Involving Information Originated by a Foreign Government or Another U.S. Government Agency. Whenever a loss or possible unauthorized disclosure involves the classified information or interests of a foreign government agency, or another government agency, the department or agency in which the compromise occurred shall advise the other government agency or foreign government of the circumstances and findings that affect their information or interests. However, foreign governments normally will not be advised of any security system vulnerabilities that contributed to the compromise.

(c) Inquiry/Investigation and Corrective Actions. Agency heads shall establish appropriate procedures to conduct an inquiry/investigation of a loss, possible compromise or unauthorized disclosure of classified information, in order to implement appropriate corrective actions, which may include disciplinary sanctions, and to ascertain the degree of damage to national security.

(d) Department of Justice and Legal Counsel Coordination. Agency heads shall establish procedures to ensure coordination with legal counsel whenever a formal action, beyond a reprimand, is contemplated against any person believed responsible for the unauthorized disclosure of classified information. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, agency heads shall use established procedures to ensure coordination with (i) the Department of Justice, and (ii) the legal counsel of the agency where the individual (s) responsible is assigned or employed.

Section X - Special Access Programs

(a) General. The safeguarding requirements for information in Special Access Programs (SAP), established under the provisions of Section 4.4 of E.O. 12958 may be enhanced by the agency head responsible for creating the SAP. Agency heads shall ensure that the enhanced controls are based on an assessment of the value, criticality, threat and vulnerability of the information.

(b) Significant Interagency Support Requirements. Agency heads must ensure that a Memorandum of Agreement/Understanding (MOA/MOU) is established for each Special Access Program that has significant interagency support requirements. These MOAs/MOUs must address support requirements and supporting agency oversight responsibilities.

Section XI - Telecommunications, Automated Information Systems and Network Security

Each agency head shall ensure that classified information electronically processed, stored or transmitted is protected in accordance with applicable national policy issuances.

Section XII - Technical Security

Based upon the risk management factors referenced in Section I of this Directive agency heads shall determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures (TSCM) and TEMPEST necessary to detect or deter exploitation of classified information through technical collection methods and may apply countermeasures in accordance with applicable national policy issuances.

Section XIII - Emergency Authority

Agency heads may prescribe special provisions for the dissemination, transmittal, destruction, and safeguarding of classified information during military operations or other emergency situations.

ANNEX A - Open Storage Areas

This Annex describes the construction standards for open storage areas.

1. Construction: The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in a manner as to provide visual evidence of unauthorized penetration.

2. Doors: Doors shall be constructed of wood, metal, or other solid material. Entrance doors shall be secured with a built-in GSA-approved three position combination lock. When special circumstances exist, the agency head may authorize other locks on entrance doors for Secret and Confidential storage. Other doors shall be secured from the inside with either deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar which extends across the width of the door, or by other means approved by the agency head.

3. Vents, Ducts, and Miscellaneous Openings: All vents, ducts, and similar openings in excess of 96 square inches (and over 6 inches in its smallest dimension) that enter or pass through an open storage area shall be protected with either bars, expanded metal grills, commercial metal sounds baffles, or an intrusion detection system.

4. Windows:

a. All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings.

b. Windows at ground level will be constructed from or covered with materials which provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Open storage areas which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by the motion detection sensors within the area.)

ANNEX B - Foreign Government Information

The requirements described below are additional baseline safeguarding standards that may be necessary for foreign government information, other than NATO information, that requires protection pursuant to an existing treaty, agreement, or other obligation. NATO classified information shall be safeguarded in compliance with United States Security Authority for NATO Instructions I-69 and I-70. To the extent practical, foreign government information should be stored separately from other classified information to facilitate its control. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container. The safeguarding standards described below may be modified if required or permitted by treaties or agreements, or for other obligations, with the prior written consent of the National Security Authority of the originating government.

1. Top Secret. Records shall be maintained of the receipt, internal distribution, destruction, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction will be witnessed.

2. Secret. Records shall be maintained of the receipt, external dispatch and destruction of foreign government Secret information. Other records may be necessary if required by the originator. Secret foreign government information may be reproduced to meet mission requirements unless prohibited by the originator. Reproduction shall be recorded unless this requirement is waived by the originator.

3. Confidential. Records need not be maintained for foreign government Confidential information unless required by the originator.

4. Restricted and Other Foreign Government Information Provided in Confidence. In order to assure the protection of other foreign government information provided in confidence (e.g., foreign government "Restricted," "Designated," or unclassified provided in confidence), such information must be classified under E.O. 12958. The receiving agency, or a receiving United States contractor, licensee, grantee, or certificate holder acting in accordance with instructions received from the United States Government, shall provide a degree of protection to the foreign government information at least equivalent to that required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to US CONFIDENTIAL information. If the foreign protection requirement is lower than the protection

required for US CONFIDENTIAL information, the following requirements shall be met:

a. Documents may retain their original foreign markings if the responsible agency determines that these markings are adequate to meet the purposes served by United States classification markings. Otherwise, documents shall be marked, "This document contains (insert name of country) (insert classification level) information to be treated as US (insert classification level)." The notation, "Modified Handling Authorized," may be added to either the foreign or United States markings authorized for foreign government information. If remarking foreign originated documents or matter is impractical, an approved cover sheet is an authorized option;

b. Documents shall be provided only to those who have an established need-to-know, and where access is required by official duties;

c. Individuals being given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet;

d. Documents shall be stored in such a manner so as to prevent unauthorized access;

e. Documents shall be transmitted in a method approved for classified information, unless this method is waived by the originating government.

5. <u>Third-country Transfers</u>. The release or disclosure of foreign government information to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.

~~JB~~
JS

MD - you have
other materials
don't you?
Please keep together.
TX

CENTRAL INTELLIGENCE AGENCY

WASHINGTON, D.C. 20505

Office of General Counsel

18 November 1997

Mr. Stephen W. Preston
Appellate Staff Deputy Assistant
Attorney General
U.S. Department of Justice
Washington, D.C. 20530

Dear Mr. Preston:

Thank you for providing us with a copy of the Civil Division's memorandum dated September 29, 1997, and the Civil Rights Division's memorandum dated October 30, 1997, concerning judicial review of security clearance determinations. Let me take this opportunity to reiterate how important we believe it is continue the long-standing and successful litigation position of the Government not to permit judicial review of security clearance determinations.

We oppose judicial review of security clearance decisions for a number of reasons, not the least of which is the recognition by the Supreme Court in the Egan case that these decisions are best left to Executive Branch security professionals and not the courts. The Civil Rights Division's latest discussion of the Webster and Egan cases in the memorandum you provided offers nothing new that would cause us to reconsider our view that security clearance determinations should be made by Executive branch officials acting pursuant to the President's Constitutional authority as Commander-in-Chief. We believe we have interpreted the Webster and Egan cases correctly. We believe the Civil Rights Division has interpreted these cases to support its view of what the law in this area *should be*. Simply put, we, and as far as we know all other departments and agencies that have responded to you on this question, strongly disagree with the views of the Civil Rights Division and the Division's proposal for judicial review of security clearance decisions.

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001a. letter	To Stephen Preston from CIA Counsel. [partial] [CIA Act] (1 page)	11/18/1997	P3/b(3)

COLLECTION:

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

FOLDER TITLE:

Personnel Security [5]

2006-1066-F
vz874

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]

In particular, as we indicated earlier, any invitation by the Executive Branch to the judiciary to review security clearance decisions would not be susceptible to meaningful limitations imposed by the Executive Branch. We also are unpersuaded by the Civil Rights Division's references to the discussion that took place at the Department's Working Group on this topic, discussions to which the Agency was not a party. We do not agree with the Civil Rights Division that there needs to be an administrative process in place "similar to the EEO procedures..." to ensure that unlawful and discriminatory security clearance practices do not occur. The Civil Rights Division has offered nothing beyond its speculation that such unlawful activities might be taking place within the U.S. Government. Moreover, we are not persuaded that the Presidentially-mandated administrative procedures for security clearance appeals would be inadequate to uncover and correct any unlawful and discriminatory security clearance decision-making.

Finally, let me add that the Director of Central Intelligence believes that security is a core function of the Agency and he remains very interested in ensuring that security clearance decisions are made by security professionals in accordance with the President's directions contained in Executive Order 12968, *Access to Classified Information*. Please keep us informed of Department's discussions on this very important topic.

Sincerely,

[001a] P3/(b)(3)

Principal Deputy General Counsel

cc: Mr. James E. Baker, NSC
Ms. Judith A. Miller, DOD
Mr. David R. Andrews, DOS
Mr. Larry Parkinson, FBI
Mr. Eric J. Fygi, DOE
Mr. Edward S. Knight, Treasury

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001b. memo	For Various from Stephen Preston. [partial] [CIA Act] (1 page)	11/05/1997	P3/b(3)

COLLECTION:

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

FOLDER TITLE:

Personnel Security [5]

2006-1066-F
vz874

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]

U.S. Department of Justice

Civil Division

Deputy Assistant Attorney General

Washington, D.C. 20530

November 5, 1997

MO

JS

Return JS

MEMORANDUM

TO: David R. Andrews
Legal Adviser
Department of State

Edward S. Knight
General Counsel
Department of Treasury

Judith A. Miller
General Counsel
Department of Defense

Eric J. Fygi
Acting General Counsel
Department of Energy

[001b] P3/(b)(3)
Central Intelligence Agency

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation

FROM: Stephen W. Preston

RE: Judicial Review of Security Clearance Determinations

We appreciate your providing the views of your respective agencies on the availability of judicial review for alleged discrimination in security clearance denials and revocations. Attached, for your information, are the Civil Division's memorandum conveying your responses and likewise expressing the view that the litigating position of the United States should remain unchanged, and the Civil Rights Division's memorandum urging adoption of the alternative position. (Please remember that these materials are privileged and that appropriate steps should be taken to maintain their confidentiality.) The matter is now under consideration.

cc: Alan Kreczko
Legal Adviser
National Security Council

U.S. Department of Justice

Civil Division

Office of the Assistant Attorney General

Washington, D.C. 20530

September 29, 1997

MEMORANDUM FOR THE DEPUTY ATTORNEY GENERAL

THROUGH: ACTING ASSOCIATE ATTORNEY GENERAL

FROM: Frank W. Hunger
Assistant Attorney General
Civil Division

RE: Judicial Review of Security Clearance Determinations

This memorandum presents the view of the Civil Division on an issue of considerable importance to the national security community, as well as litigating components of the Department of Justice.

The availability of judicial review for alleged discrimination in security clearance denials and revocations has been a focus of discussion within the Department and elsewhere for some time, principally in connection with matters in litigation. To date, in cases brought under Title VII or directly under the Constitution, the Civil Division has taken the position that there is no judicial review for claims of discrimination in security clearance determinations. At the same time, others have voiced concern about this position, urging that the government should acknowledge some form of judicial review for such discrimination.

In order to facilitate an examination of the litigating position of the United States in this regard, an informal DOJ working group was convened under the auspices of the Deputy Attorney General and charged with formulating — for discussion and, if appropriate, further consideration — a possible alternative to the existing position. The enclosed discussion paper reflects the work of the group (TAB 1). It describes an approach "that aims to permit limited judicial review of security clearance determinations while minimizing the risks to national security." The paper concludes, "[a]lthough some members continue to have substantial reservations about the ultimate wisdom of adopting this proposal as the Department's new litigating position, the working group believes it has sufficient merit to warrant discussion with the national security agencies."

At the end of May, we distributed the discussion paper to the chief legal officers of the principal national security agencies for comment. We have since received responses from the Department of State (TAB 2), the Department of the Treasury (TAB 3), the Department of Defense (TAB 4), the Central Intelligence Agency (TAB 5) and the Federal Bureau of Investigation (TAB 6).[1] These agencies are unanimous, and quite adamant, in their opposition to any change in the litigating position of the United States in this regard and, specifically, to adoption of the alternative approach described in the discussion paper.

In light of the concerns of our client agencies, and for reasons previously articulated, we cannot support adoption of the alternative approach described in the discussion paper.

- The alternative approach is not legally compelled. To the contrary, our existing position is consistent with applicable Supreme Court decisions and has been sustained by every court of appeals to address it.

- Our existing position serves to preserve Executive prerogatives and to protect the national security. If we were to advocate the alternative approach, there is no assurance whatsoever that the courts would confine themselves to a form of judicial review so limited. Thus a change in position could yield greater incursion on Executive prerogatives and greater risk to the national security.

- Discrimination in security clearance determinations is expressly prohibited by Executive Order. If there is evidence of unredressed discrimination — we are aware of none — the focus should be on ensuring adequate administrative procedures and remedies, not on creating rights to judicial review that are otherwise problematic.

Accordingly, we continue in the view that the litigating position of the United States — that there is no judicial review for claims of discrimination in security clearance determinations — should remain unchanged. At the outset of this examination, we identified two paramount interests: the interest in preventing discrimination in security clearance determinations and in rectifying any such discrimination that occurs, and the interest in protecting the national security and in preserving the President's constitutional authority in this area. We believe that the existing litigating position, together with the faithful implementation through effective administrative

---

[1] The Department of Energy has not responded.

processes of the prohibition against discrimination in Exec. Order No. 12,968, best reconciles these interests and fully accommodates each of them.[2]

cc: David W. Ogden

---

[2] In the event of further discussion, the National Security Council, Legal Adviser, has indicated that he would like an opportunity to participate.

U.S. Department of Justice

Civil Rights Division

Office of the Assistant Attorney General

Washington, D.C. 20035

OCT 30 1997

MEMORANDUM FOR THE DEPUTY ATTORNEY GENERAL

THROUGH: ACTING ASSOCIATE ATTORNEY GENERAL

FROM: Isabelle Katz Pinzler
Acting Assistant Attorney General
Civil Rights Division

SUBJECT: Judicial Review of Employment Actions Based On Security Clearances

In 1995, the Civil Division and the Civil Rights Division began discussing the United States' position in Title VII employment discrimination cases in which government employees claimed that they were denied security clearances for discriminatory reasons. Until that time, the Civil Division had been arguing successfully in the district courts and the courts of appeals that courts have no jurisdiction to hear federal employees' claims of discrimination in security clearance determinations in cases brought under either Title VII or the Constitution. The Civil Rights Division's position was that the denial of all judicial review was not only unsupported by Supreme Court precedent, but also poor policy.

The Deputy Attorney General's office formed an intradepartmental Working Group in early 1996 to address the issue. The Working Group was chaired by David Ogden and included representatives from the Civil Division, the Civil Rights Division, the FBI, the Office of the Solicitor General, and the Office of Policy Development, and the Office on Intelligence Policy and Review. The Working Group ultimately formulated a compromise proposal stating that while there would be no Title VII review of employment actions based on denials or revocations of security clearances, there would be limited judicial review under the APA of claims that discrimination in employment actions based on security clearance determinations violated the Constitution. In mid-1997, the Civil Division circulated the proposal to agencies with a particular interest in national security issues for their comments.

We have received memoranda from the State Department, FBI, CIA, Defense Department, and Treasury Department, along with the memorandum from the Civil Division, discussing the Working

Group's compromise proposal. Each of the memoranda essentially takes the same position, opposing the compromise position that the Working Group developed.

The Civil Rights Division strongly recommends that the Department adopt the litigating position set forth in the compromise proposal. Under the agencies' view, all acts of racial or sexual discrimination by a security clearance adjudicator would be immune from review, even if the adjudicator admitted that the decision was made for discriminatory reasons. We do not think that this is an accurate statement of the law, nor is it an appropriate position for the United States to be asserting as a policy matter.

1. The agencies and the Civil Division memorandum rely on Department of the Navy v. Egan, 484 U.S. 518 (1988) to argue that security decisions are totally immune from judicial review. Egan, however, did not involve a constitutional claim; rather, the issue was whether the Merit Systems Protection Board had statutory jurisdiction to review the merits of security clearance determinations. Indeed, the compromise position follows Egan's holding that judicial review of employment actions based on security concerns is not permitted absent an express Congressional indication in the statute to permit that review. The Working Group agreed, relying on Egan, that we would not seek to assert Title VII jurisdiction over these claims because there is no such direct statutory language in Title VII permitting review of employment actions based on security clearances.

The view that Egan totally eliminates any form of judicial review of constitutional claims, however, cannot be squared with the Supreme Court's later decision in Webster v. Doe, 486 U.S. 592 (1988). Webster explicitly held that even in the national security context, a "serious constitutional question" would be raised by any congressional attempt to preclude judicial review of constitutional claims. Webster held that a CIA employee could pursue a claim that he was fired for being gay, and that the termination of his employment violated his constitutional rights. The Court in Webster specifically rejected the government's argument (which is essentially repeated in the memoranda opposing the compromise position) that "all Agency employment termination decisions, even those based on policies normally repugnant to the Constitution, are given over to the absolute discretion of the Director, and are hence unreviewable under the APA." 486 U.S. at 603. The Court concluded that "[n]othing in section 102(c)[of the National Security Act] persuades us that Congress meant to preclude consideration of colorable constitutional claims arising out of action of the Director pursuant to that section; we believe that a constitutional claim based on an individual discharge may be reviewed by the District Court." In our view, it could not be much clearer that Webster holds that a claim that employment action based on an unconstitutional security clearance decision is reviewable in federal court.

Although the agencies attempt to distinguish Webster as an employment case, and not a security clearance case, at issue in Webster was the substance of the CIA's decision to terminate the plaintiff's employment because of national security concerns. The Supreme Court has never held that any administrative decisions -- even those involving national security -- are wholly exempt from judicial scrutiny, and did not make such a holding in Egan.

This judicial approach is not limited to Webster. In Nat'l Federation of Federal Employees v. Greenberg, 983 F.2d 286, 289-290 (D.C. Cir. 1993), the court rejected the view that the President's constitutional power as commander-in-chief under Article II prevented any review of matters relating to the granting of security clearances. The court noted that "a large measure of discretion gives rise to judicial deference, but not immunity from judicial review of constitutional claims." 983 F.2d at 290.[1/] Indeed, Greenberg specifically stated that Webster "undercuts" the government's argument that Egan can be read to eliminate federal court review of "all security clearance decisions," holding instead that "[i]t is simply not the case that all security-clearance decisions are immune from judicial review." 983 F.2d at 289.

2. The agencies argue that judicial review of discrimination claims is unnecessary because existing administrative procedures are an adequate substitute. Executive Order 12968, Sec. 3.1(c)(1995), provides that "[t]he United States Government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information," and the agencies suggest that this Executive Order provides employees with adequate protection from acts of discrimination.

The discussions held in the Working Group do not support this claim. The explanation of the agency review of security

---

[1/] The Department of the Treasury's reliance on American Federation of Government Employees v. HUD, 118 F.3d 786, 794 (1997) is misplaced. The court in that case did not address the issue of judicial review of constitutional violations in employment decisions that involve security clearances. The court refused to prohibit the Department of Defense from asking about mental health treatment on its security clearance questionnaire, "consistent with our traditional reluctance to intrude on Executive decisionmaking in the area of national defense," and held that the employee's right to privacy was not violated by the agencies' legitimate need for this information.

denials given to the Working Group was that the Executive Order set up a system for review of security clearance denials in which the denial was reviewed by another level of agency personnel. The Working Group was also told that the employee could allege that the denial was racially motivated, but there was no mechanism under which the employee could present evidence about action on other security clearances to show disparate treatment. Any claim of discrimination would require examination of actions taken with respect to others in similar circumstances. The comparison of the treatment of members of different races (or genders) is essential if there is really going to be a complete assessment of whether a particular action was discriminatory. While there was an indication that agencies might eventually set up such a system, it was also clear that, at the time we met, there was no such system in place anywhere. For the Department to decide that judicial review is unnecessary to protect individuals from discrimination because we have an administrative mechanism requires, in our view, that a real mechanism be in place, and the discussions we had indicated that this had not yet occurred.

In the absence of a directive to agencies that they consider evidence of discrimination in the denial of a security clearance, including statistical and other evidence that similarly-situated individuals were granted clearances, the administrative process will not serve as any kind of substitute -- let alone an adequate one -- for judicial review of constitutional claims. Agencies must establish a system explicitly designed to consider discrimination claims in the security clearance process to ensure compliance with the Executive Order, similar to the EEO procedures agencies have in place to deal with claims of discrimination in the employment context.

This form of administrative review also is essential if we go to court under APA review. As we discussed in the Working Group, the court's function in this kind of case would be to review the administrative record to see that the agency's finding of no discrimination is correct. However, in our view, an administrative mechanism does not erase the need for judicial review of constitutional claims of discrimination in the security clearance context.

3. The agencies' concern that some judges may not limit discovery into the security clearance determination process as the proposal envisions may have merit. Under the compromise proposal intended, APA review is limited to the administrative record. As we discussed in the Working Group, the creation of a full administrative record is critical to the argument that APA review is limited to that record, and will eliminate any need for discovery.

It is simply not realistic to think that courts will assume the right to determine who should receive a security clearance. Both district courts and courts of appeals have been remarkably willing to accede to claims that they should not interfere in national security matters, and it is difficult to understand why courts would be less willing to agree to limited review when they have acceded so often to no review at all. While there is a chance that a district court judge will attempt to interfere unduly with the agencies' prerogatives, the possibility of incorrect action on the part of a lower court judge should not drive the government's policy. The Supreme Court noted in Webster that even without a statutory withdrawal of the power to consider claims in this area, "traditional equitable principles requiring the balancing of public and private interests control the grant of declaratory or injunctive relief in the federal courts." 486 U.S. at 604 (citations omitted). Such principles have protected the executive branch from interference with its national security functions in the past, and ensuring that those functions are exercised in a nondiscriminatory fashion will not harm legitimate national security interests.

It is important to remember that permitting judicial review of allegations of discrimination does not envision courts reviewing the specific criteria on which security decisions are made and deciding that the criteria are improper. The allegation of discrimination is that others of different races or genders have been treated differently; in other words, that the same criteria have not been applied similarly to all persons. Nowhere does the compromise position envision that courts will be determining that the criteria are themselves discriminatory.

4. The agencies also assert that the officers assigned to determine security clearances will feel pressure to grant clearances they otherwise would have denied simply because there is the possibility of judicial review of their decisions. We certainly defer to the security agencies' knowledge of the actions of their own employees. We are dubious, however, that an employee who has the grave responsibility of deciding who should get a security clearance will decide to grant a questionable clearance simply to avoid the possibility of a federal court challenge to that decision, particularly when the agency, and not the employee, will be defending the decision.

5. A number of the memoranda also suggest that discrimination in the denial or revocation of clearances is simply not a problem. No one, during the creation of the compromise proposal, suggested that it is a widespread problem. Of course, since there is no judicial review, and until now no mechanism for administrative review, it is hard to know whether it is a problem or not. In any event, the adoption of the legally correct position permitting limited judicial review should not be dependent on a finding that racial and sexual

discrimination in the granting of security clearances is a widespread problem.

6. None of the agency memoranda appear to acknowledge one principle that was important in the creation of the compromise proposal -- the concern with the Justice Department taking the position that employees who may have been subject to race or sex discrimination in the denial or revocation of a security clearance, and therefore a job, simply have no judicial recourse. In addition to the fact that the Webster decision strongly indicates that our present legal position is incorrect, the fact is that the present litigating position of the Administration is denying all judicial recourse to possible victims of government racial or sexual discrimination.

cc: Assistant Attorney General
Civil Division

Legal Adviser
Department of State

General Counsel
Department of Defense

General Counsel
Department of the Treasury

General Counsel
Central Intelligence Agency

General Counsel
Federal Bureau of Investigation

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
002. memo	For Alan Kreczko from Charles Ruff. Subject: Clearances. (1 page)	04/08/1997	P6/b(6)

COLLECTION:

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

FOLDER TITLE:

Personnel Security [5]

2006-1066-F
vz874

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
NSC/RMO PROFILE

RECORD ID: 9720323
RECEIVED: 18 APR 97 15

TO: HALL, J

FROM: DAVIES

DOC DATE: 22 APR 97
SOURCE REF:

KEYWORDS: SECURITY ACCESS

PERSONS: LAKE, T

SUBJECT: SECURITY CLEARANCE CERTIFICATION - TONY LAKE

Please file:
→ Security
TX.

ACTION: DAVIES SGD MEMO
DUE DATE: 22 APR 97
STATUS: C

STAFF OFFICER: BAKER
LOGREF:

FILES: NS
NSCP:
CODES:

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

FOR ACTION	FOR CONCURRENCE	FOR INFO
		BAKER
		KRECZKO
		LEARY
		NSC CHRON

COMMENTS:

DISPATCHED BY ________________ DATE ________ BY HAND W/ATTCH

OPENED BY: NSTMH
CLOSED BY: NSMEC
DOC 2 OF 2

UNCLASSIFIED

20323

April 18, 1997

ACTION

MEMORANDUM FOR GLYN T. DAVIES

THROUGH: ALAN KRECZKO AK

FROM: JAMES E. BAKER JB

SUBJECT: Tony Lake's Security Clearances

Jim Hall, Bill Leary and I have prepared the attached document to formally record that Mr. Lake is retaining his clearances in anticipation that there will be a need for official consultation. Although the paper trail is somewhat scant, we understand that it is standard practice for National Security Advisors to retain their clearance after departing. However, there appears to be no formal written documentation from past administrations to record this step. We believe a formal record that Mr. Lake is retaining his clearances should be kept so that the NSC Security Officer is in a position to certify Mr. Lake's clearance to other agencies when need be and to periodically have it updated as required. "Need to know" determinations will continue to be made by those responsible for the information in question.

We have shown the attached memorandum to Mr. Lake and cleared it in substance with Steve Garfinkel, Director of the Information Security Oversight Office. Steve concurs in our approach.

Concurrence by: Bill Leary and Jim Hall

RECOMMENDATION

That you sign the memorandum at Tab I.

Attachment
Tab I Clearance Memorandum

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
003a. memo	For James Hall from Glyn Davies. Subject: Anthony Lake's Clearance Certification. [partial] (1 page)	04/22/1997	P6/b(6)

COLLECTION:

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

FOLDER TITLE:

Personnel Security [5]

2006-1066-F
vz874

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]

WASHINGTON, D C 20504

April 22, 1997

MEMORANDUM FOR JAMES HALL

FROM: GLYN T. DAVIES

SUBJECT: Security Clearance Certification -- W. Anthony K. Lake

Pursuant to the provisions of Executive Order 12968 and standards contained in Director of Central Intelligence Directive 1/14, I have determined that you are authorized to maintain the clearance of Mr. Anthony Lake, formerly Assistant to the President for National Security Affairs. This clearance is necessary for the accomplishment of official governmental purposes, subject to appropriate need to know determinations being made on a case-by-case basis.

When requested, you shall certify to other departments and agencies of the executive branch, and to the private sector, the level of security clearance granted Mr. Lake by the NSC.

[003a] P6/(b)(6)

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
003b. draft	For James Hall from Glyn Davies. Subject: Anthony Lake's Clearance Certification. [partial] (1 page)	04/22/1997	P6/b(6)

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

FOLDER TITLE:
Personnel Security [5]

2006-1066-F
vz874

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]

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

20323

JAMES HALL
MEMORANDUM FOR ~~DIRECTOR, NSC SECURITY PROGRAM~~
FROM: Glyn T. Davies
SUBJECT: Security Clearance Certification -- W. Anthony K. Lake

Pursuant to the provisions of Executive Order 12968 and standards contained in Director of Central Intelligence Directive 1/14, I have determined that you are authorized to maintain the clearance of Mr. Anthony Lake, formerly Assistant to the President for National Security Affairs. This clearance is necessary for the accomplishment of official governmental purposes, subject to appropriate need to know determinations being made on a case-by-case basis.

When requested, you shall certify to other departments and agencies of the executive branch, and to the private sector, the level of security clearance granted Mr. Lake by the NSC.

[003b] P6/(b)(6)

~~Glyn T. Davies~~
~~Executive Secretary~~

RECORD ID: 9720323

ACTION DATA SUMMARY REPORT

DOC	ACTION OFFICER	CAO	ASSIGNED	ACTION REQUIRED
001	DAVIES	Z	97042110	FOR SIGNATURE
002		X	97042208	DAVIES SGD MEMO

DISPATCH DATA SUMMARY REPORT

DOC	DATE	DISPATCH FOR ACTION	DISPATCH FOR INFO
002	970422	HALL, J	

NATIONAL SECURITY COUNCIL

SECURITY AWARENESS BULLETIN

ALL EMPLOYEES: NSC January 31, 1997

Cordell Hull Conference Room

The Cordell Hull Conference Room (208 OEOB) is a Sensitive Compartmented Information Facility (SCIF). Anyone scheduling this facility must hold Sensitive Compartmented Information (SCI) security clearances (TS/SI/TK/G). Authorized personnel who permit another individual(s) to enter this area are responsible for confirming the individual's security clearances and need-to-know. Guests without SCI clearances must be escorted at all times and should never be left alone. Finally, the hallway door should remain closed after the meeting starts.

It is the users responsibility to ensure that no classified materials remain in the area. All audio/video equipment should be turned off and the entrance/exit door immediately secured upon departure.

The Systems and Technical Planning Directorate is reponsible for the scheduling and technical assistance for the Codell Hull Conference room. If you need to use this facility or require quidance with equipment needs, please contact SYS/TECH PLANNING, 456-9311.

NSC/Security can provide you with individual security quidance and answer any questions you may have. Please direct any security related issues, to include security clearance verification to Jim Hall on 456-9308.

Office of Origin: National Security Council
Security Programs

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

20323

April 18, 1997

ACTION

MEMORANDUM FOR GLYN T. DAVIES

THROUGH: ALAN KRECZKO AK

FROM: JAMES E. BAKER JB

SUBJECT: Tony Lake's Security Clearances

Jim Hall, Bill Leary and I have prepared the attached document to formally record that Mr. Lake is retaining his clearances in anticipation that there will be a need for official consultation. Although the paper trail is somewhat scant, we understand that it is standard practice for National Security Advisors to retain their clearance after departing. However, there appears to be no formal written documentation from past administrations to record this step. We believe a formal record that Mr. Lake is retaining his clearances should be kept so that the NSC Security Officer is in a position to certify Mr. Lake's clearance to other agencies when need be and to periodically have it updated as required. "Need to know" determinations will continue to be made by those responsible for the information in question.

We have shown the attached memorandum to Mr. Lake and cleared it in substance with Steve Garfinkel, Director of the Information Security Oversight Office. Steve concurs in our approach.

Concurrence by: Bill Leary and Jim Hall

RECOMMENDATION

That you sign the memorandum at Tab I.

Attachment
Tab I Clearance Memorandum

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
004. memo	Duplicate of 003a. (1 page)	04/22/1997	P6/b(6)

COLLECTION:

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

FOLDER TITLE:

Personnel Security [5]

2006-1066-F
vz874

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]

20323

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

MEMORANDUM FOR DIRECTOR, NSC SECURITY PROGRAM

SUBJECT: Security Clearance Certification -- W. Anthony K. Lake

Pursuant to the provisions of Executive Order 12968 and standards contained in Director of Central Intelligence Directive 1/14, I have determined that you are authorized to maintain the clearance of Mr. Anthony Lake, formerly Assistant to the President for National Security Affairs. This clearance is necessary for the accomplishment of official governmental purposes, subject to appropriate need to know determinations being made on a case-by-case basis.

When requested, you shall certify to other departments and agencies of the executive branch, and to the private sector, the level of security clearance granted Mr. Lake by the NSC.

[004] P6/(b)(6)

Glyn T. Davies
Executive Secretary

- JB/JS
- Jim Hall
- File

U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535

KL
Alan K

November 6, 1996

Mr. John M. Quinn
Counsel to the President
The White House
Washington, D.C.

Dear Mr. Quinn:

This responds to a request by Mr. Charles C. Easley, Executive Office of the President (EOP) Security Officer, Office of Administration, that the FBI consent to copying by the CIA of personnel investigation materials provided by the FBI to White House units, for the purpose of facilitating CIA's adjudication of access eligibility for Sensitive Compartmented Information (SCI).

The cognizant White House (including EOP) unit has FBI authorization (absent notification to the contrary) to make available to authorized CIA personnel investigation materials provided to the White House unit by the FBI, if the cognizant White House unit determines that such CIA personnel have a legitimate need to have the information for the purpose of adjudicating a person's eligibility for SCI access, and if such disclosure is not otherwise precluded by applicable laws or regulations. Under this authorization, the cognizant White House unit may in its discretion provide CIA personnel with photocopies of these materials, provided that CIA agrees and will ensure that all photocopies so furnished will be returned to the cognizant White House unit within ninety (90) days of being provided the photocopies and that any derivative photocopies thereof which CIA might make are destroyed within this ninety-day period.

Please do not hesitate to let me know if my office can be of assistance in resolving future issues which may surface. For staff coordination, my primary point of contact is William Miller of this unit. Either of us may be reached at (202) 324-4523.

Sincerely,

Patrick W. Kelley

Patrick W. Kelley
Assistant General Counsel
Administrative Law Unit